Contents

- Microsoft Edge Enterprise documentation
- Microsoft Edge documentation
- Get started with Microsoft Edge
  - Learn about Microsoft Edge Channels
  - See what's new
  - Customer adoption materials
  - Explore documentation resources
  - Microsoft Edge hands-on deployment lab
  - Windows Blogs - Microsoft Edge Developer
  - Microsoft Edge FAQ
- Plan for Microsoft Edge
  - Microsoft Edge Enterprise Roadmap
  - Platform support for Microsoft Edge features
  - Plan your deployment of Microsoft Edge
  - Microsoft Edge in your environment
  - Microsoft browser usage report
  - Ready for Microsoft Edge
  - Mobile Stable Channel Release Notes
  - Stable Channel Release Notes
  - Stable Channel archived release notes
  - Beta Channel Release Notes
  - Beta Channel archived release notes
  - Release schedule
  - Security updates
  - Supported Operating Systems
  - Lifecycle Policy
  - Supported languages
  - System updates for Microsoft Edge
    - Windows updates to support Microsoft Edge

- Deploy Microsoft Edge
  - Deploy Microsoft Edge with Windows 10 updates
  - Deploy to Windows with Configuration Manager
  - Deploy to Windows with Intune
  - Deploy to macOS with Jamf
  - Deploy to macOS with Intune
- Configure Microsoft Edge
  - Configure for Windows with group policies
  - Configure for Windows with Intune
  - Configure Microsoft Edge using Initial Preferences settings for the first run
  - Per-site configuration by policy
  - Configure for Windows with Mobile Device Management
  - Configure for macOS using a .plist
  - Configure for macOS with Jamf
- Use Microsoft Edge enterprise features
  - Microsoft Edge Workspaces
  - Microsoft Edge for Virtual desktop infrastructure
  - Configurations and experimentation
  - Enterprise new tab page
  - Identity support and configuration
  - Microsoft Edge and Enterprise State Roaming
  - Plan your kiosk mode transition
  - Configure Microsoft Edge kiosk mode
  - Manage Microsoft Edge extensions
    - Manage extensions in the enterprise
    - Manage the sidebar in Microsoft Edge
    - Use group policies to manage extensions
    - Self-host Microsoft Edge extensions
    - Detailed guide to the ExtensionSettings policy
    - Extensions FAQ
  - Microsoft Edge enterprise sync
    - Configure Microsoft Edge sync

- Diagnose and fix Microsoft Edge sync issues
- Sync FAQ
- On-premises sync for Active Directory users
- PDF reader in Microsoft Edge
- Set Microsoft Edge as the default browser
- Split tunnel VPN support for WebRTC
- Use Microsoft Edge in Internet Explorer mode
  - What is Internet Explorer (IE) mode?
  - Enterprise site configuration strategy
  - Configure IE mode Policies
  - Cloud Site List Management for Internet Explorer (IE) mode
  - IE Mode Local Site List
  - Disable Internet Explorer 11
  - Site Discovery and list management
    - Enterprise Site Discovery Step-by-Step Guide
    - Enterprise Site List Manager in Microsoft Edge
  - Keep in-page navigation in IE mode
  - Cookie sharing between Microsoft Edge and Internet Explorer
  - Configurable sites in IE mode
  - Associate file extensions with Internet Explorer mode
  - IE mode troubleshooting and FAQ
- Microsoft Edge Security
  - Security for your business
  - Modern security protection for vulnerable legacy apps
  - Browse more safely with Microsoft Edge
  - Identify and interrupt downloads of potentially dangerous files
  - Allow list for Microsoft Edge endpoints
  - Data Loss Prevention (DLP)
  - Password Monitor auto-enabled for users
  - Microsoft Edge password manager security
  - Protect against potentially unwanted applications
  - Support for Azure AD Conditional Access

- Support for Application Guard
- Support for Microsoft Defender SmartScreen
- Support for Windows Information Protection
- Microsoft Edge Privacy
  - Configure privacy settings
  - Microsoft Edge Privacy Whitepaper
- Microsoft Edge Reference
  - Browser policy reference
  - Update policy reference
  - WebView2 policy reference
  - Learn more reference
    - Backwards compatibility for Enterprise New tab page
    - Block access to consumer accounts
    - ClickOnce and DirectInvoke
    - Command-line options to configure proxy settings
    - Configurable Microsoft Edge commands
    - Filter format for URL list-based policies
    - Microsoft Edge will disable modifying document.domain
    - Mixed content downloads
    - Progressive rollouts for Stable channel updates
    - Provision favorites for Microsoft Edge
    - Redirection from Internet Explorer to Microsoft Edge
    - Regular Expression 2 (re2.h) syntax
    - Reset Microsoft Edge data in the cloud
    - User data directory variables
    - Using Microsoft Edge rollback for enterprises
- Microsoft Edge Videos
  - Microsoft Edge video collection
  - Video - Microsoft Edge - State of the browser 2020
  - Video - Browser isolation using Application Guard
  - Video - Deploy Microsoft Edge
  - Video - Data loss prevention (DLP)

Video - Identity in Microsoft Edge

Video - Microsoft Edge version rollback

Video - PDF reader in Microsoft Edge

Video - Secure browsing on Microsoft Edge

Video - Security, compatibility, and manageability

Overview of the Microsoft Edge channels

11/1/2022 • 7 minutes to read • Edit Online

One of the benefits of the next version of Microsoft Edge is that Microsoft can provide new features regularly. However, as the admin who deploys Microsoft Edge to users in your organization, you might want more control over how often your users get these new features. Microsoft provides four options, called channels, to control how often Microsoft Edge is updated with new features. Here's an overview of the four options.

For more information on support for each channel, read: Microsoft Edge Lifecycle

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

Channel overview

CHANNEL	PRIMARY PURPOSE	HOW OFTEN UPDATED WITH NEW FEATURES	SUPPORTED?
Stable	Broad Deployment	~4 weeks	Yes
Extended Stable	An enterprise release option for Stable aligned to a longer release cycle	~8 weeks	Yes
Beta	Representative validation in the organization	~4 weeks	Yes
Dev	Planning and developing	Weekly	No
Canary	Bleeding edge content	Daily	No

The update channel you decide to deploy depends on several factors. For example, the number of line-of-business applications in use will affect your testing requirements every time there's a Microsoft Edge update. To help you make this decision, review the following information about the four update channels that are available for Microsoft Edge.

Stable Channel

The Stable Channel is intended for broad deployment in your organization, and it's the channel that most users should be on. It's the most stable of the channels and is the result of the stabilization of the feature set available in the prior Beta Channel release. New features ship about every 4 weeks. Security and quality updates ship as needed. A release from the Stable Channel is serviced until the next release from the channel is available.

Beta Channel

The Beta Channel is intended for production deployment to a representative sample set of users. It's a supported release, and each release from Beta is serviced until the next release is available. This channel provides a great opportunity to validate that things work as expected in your environment. If you find an issue, it can be remediated before the release is published to the Stable Channel. New features ship about every 4 weeks. Security and quality updates ship as needed.

Dev Channel

The Dev Channel is intended to help you plan and develop with the latest capabilities of Microsoft Edge, but with higher quality than the Canary Channel. This channel is your opportunity to get an early look at what is coming next and prepare for the next Beta release.

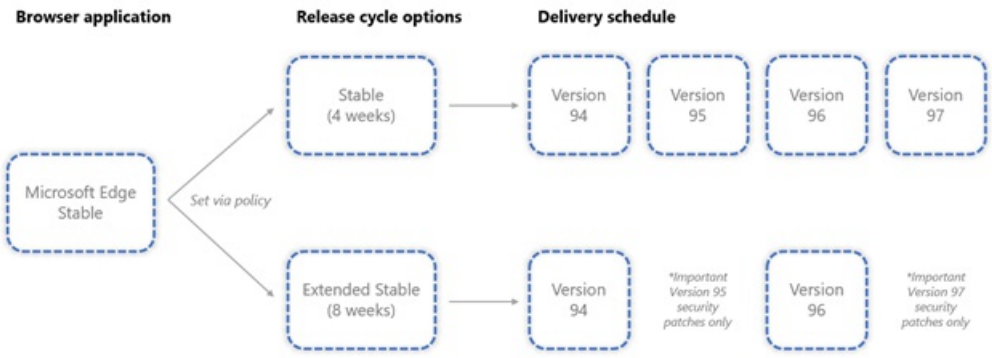
Canary Channel

The Canary Channel ships daily and is the most bleeding edge of all the channels. If you want access to the newest investments, they'll appear here first. Because of the nature of this cadence, problems will arise over time. You may want another channel installed side by side if you're using the Canary releases.

Extended Stable Channel

Unlike our preview channels (Canary, Dev, and Beta), the Extended Stable Channel isn't available as a separate browser application. This channel is an enterprise release option for the Microsoft Edge Stable application that's aligned to a longer, 8-week major release cycle. This option is opposed to the 4-week major release cycle for the Stable channel. While we recommend updating Stable on its 4-week release cycle, Extended Stable exists to more effectively serve organizations that may require a longer timeline to test and validate new browser versions.

The 8-week "Extended Stable" release option for Microsoft Edge Stable delivers cumulative feature updates that align with *even-numbered* releases beginning with Microsoft Edge 94. Feature updates from odd-numbered releases will be packaged and delivered as part of the subsequent even-numbered release. For example, if an organization selects the 8-week "Extended Stable" release cycle with Microsoft Edge 94, they'll get subsequent feature updates with Microsoft Edge 96, Microsoft Edge 98, and so on. While feature updates are packaged and delivered with new version releases based on the selected release cycle, important security patches and fixes will be delivered as needed. These security updates are independent of the selected release option to help maintain browser security. Customers can opt into the Extended Stable release option at any time, and it will take effect with the next Extended Stable release.



Opting in to the Extended Stable Release Cadence

Opting in to Extended Stable on Windows with Automatic Updates (recommended)

If you automatically update Microsoft Edge, you can use group policy objects to opt in to the Extended Stable Release Cadence. Follow this guide for more information on downloading and installing the latest Microsoft Edge Group Policy administrative templates.

1. Open the local Group Policy Editor and go to *Computer Configuration>Administrative Templates>Microsoft Edge Update>Applications>Microsoft Edge>*.
2. Select **Target Channel override** and then select **Enabled**.
3. Under **Options**, pick **"Extended Stable"** from the Policy dropdown list.

When the next update to the Extended Stable channel is released that has a version number higher than what your device currently has installed, Microsoft Edge will automatically update onto the Extended Stable channel. The version string on `edge://settings/help` will indicate that you're running a different channel.

> **NOTE**
>
> Opting-in to Extended Stable will take effect when there is a new update on the Extended Stable channel with a larger version number (major or minor) than what is currently installed on your device. If you are running the latest version of Microsoft Edge Stable and opt-in to Extended Stable, it will take effect with the next patch or update of Microsoft Edge.
>
> By default, Microsoft Edge will not downgrade itself. If you are currently running an odd-numbered version of Microsoft Edge Stable, opting-in to Extended Stable will mean that you will receive NO updates until the next even-numbered Microsoft Edge release.
>
> If you want to ensure that all of your devices start with a specific version of Extended Stable, you can deploy that specific version of Edge Stable as an MSI with rollback enabled. For example, if you want to start with Extended Stable 94 but some devices have already updated to Stable 95, you can deploy an MSI of Edge 94 with rollback enabled. For more information on how to deploy Edge MSIs with rollback enabled, see our rollback guide.

Opting in to Extended Stable on Windows via Intune

Microsoft Edge Administrative Templates can be managed similarly to local Group Policy Objects from the Microsoft Endpoint Manager admin center. Follow our guide on configuring Microsoft Edge with Intune.

The "**Target Channel override**" setting can be found under the "*Microsoft Edge Update >Applications>Microsoft Edge*" subfolders. It should be set to "**Extended Stable**"

When the next update to the Extended Stable channel is released that has a version number larger than what your device currently has installed, Microsoft Edge will automatically update onto the Extended Stable channel. The version string on `edge://settings/help` will indicate that you're running a different channel.

Opting in to Extended Stable on Windows via Configuration Manager

Refer to our guide on updating Microsoft Edge with Configuration Manager for more information on how to synchronize and approve Microsoft Edge updates in Configuration Manager.

Extended Stable updates are distributed in the software library under the "Microsoft Edge" product category, similar to existing updates for the Stable, Beta, and Dev channels. However, unlike Beta and Dev, which apply to their own browser applications, the Extended Stable updates apply to Microsoft Edge Stable application. Therefore, for your Windows Update client to determine whether to apply Stable or Extended Stable updates, it checks the status of the "Target Channel override" group policy. If the policy isn't configured or is set to "Stable," Stable updates will apply. If it's set to "Extended Stable," then Extended Stable updates will apply. Follow the instructions above for opting in to Extended Stable with Automatic Updates for instructions on how to properly set the Group Policy.

> **NOTE**
>
> If you use Configuration Manager or MSI packages to install an Extended Stable update, the page at *edge://settings/help* will not indicate that Extended Stable channel is in use. This page will only show Extended Stable as the channel name when EdgeUpdate is used to update Microsoft Edge.

Flighting Pre-release Channels in your Organization

The "Target Channel override" group policy can also be used to seamlessly flight pre-release channels of Microsoft Edge in your organization without your users needing to use a second web browser application. For example, you can set the "Target Channel override" policy to "Beta" for a representative sample set of users in your organization. When those users open Microsoft Edge, they'll be running the Beta channel release rather than Stable (probably without even realizing it!). This policy setting can give you an early insight into how the next version of Microsoft Edge will perform in your enterprise and help validate that everything works as expected. You'll get early signals from your users who encounter any issues and can ensure they're remediated prior to the release being published to the Stable Channel. As a part of troubleshooting a user's problem, the

version string at *edge://settings/help* will inform you if the user's channel is different than the default Stable channel.

> **NOTE**
>
> Since build on the "Beta" and "Dev" channels of Microsoft Edge have major version numbers larger than that of "Stable," if you take an update to the "Beta" or "Dev" channel and wish to revert back to Stable, Microsoft Edge's rollback feature will be required. Simply setting "Target Channel override" back to Stable will mean you will receive NO updates until the latest Stable release has a greater version number than the version of Microsoft Edge you are presently running on your device.

See also

- Microsoft Edge Enterprise landing page
- Channel downloads

Customer adoption materials for Microsoft Edge

11/1/2022 • 2 minutes to read • Edit Online

To support the deployment and adoption of Microsoft Edge, see the following collected materials and resources. A zip file of these materials and resources is provided for you to download.

Check back for more materials as they're made available.

Customer adoption kit

The customer adoption kit contains the following material:

- Internet Explorer Retirement Kit **(Available in English, German, Spanish, French, Japanese, Korean, Chinese (Simplified))**
  - Adoption emails
  - Flyers
  - Infographic
  - Site Collection Form
- General Adoption Kit
  - IT Deployment Guide
  - How to Get Started User Guide
  - Adoption Email Templates
  - Banners
  - Digital Signage
  - One-Pagers
  - Demo Video and GIFs
  - Web Resource Links

The adoption kit is available in English and several other languages, including French, German, and Japanese. Select your preferred language at the Microsoft Edge Customer Adoption Kit download center.

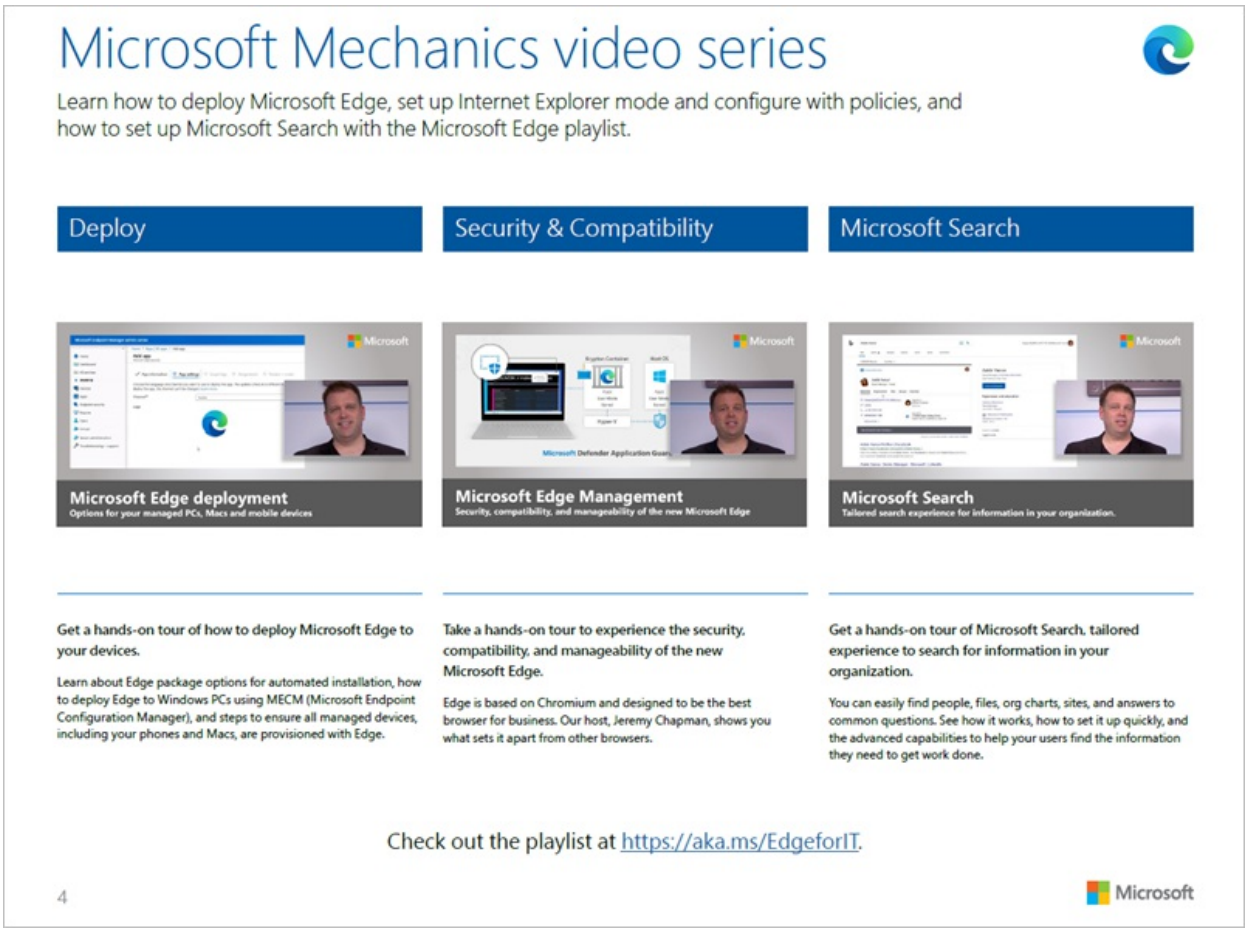
Internet Explorer (IE) Retirement Resources

Find valuable resources and expert guidance to help your organization safely and quickly move from IE to Microsoft Edge.

Microsoft Edge
Internet Explorer (IE) Retirement
Adoption Kit Overview
This kit of emails, flyers, and other resources is designed to help your organization move from Internet Explorer to Microsoft Edge. The timeline outlines how you can approach the transition—materials found in the kit are mentioned in (blue).
Phase 1: Planning
Plan: Complete internal planning process and confirm your in-org retirement date for Internet Explorer
Inform: Recruit an executive stakeholder to help transition the organization to Microsoft Edge (Executive Stakeholder Email 1)
Phase 2: Set up and pilot
Recruit: Recruit a group of core stakeholders to help pilot Microsoft Edge and IE mode before transitioning the organization (Executive Stakeholder Email 2)
Pilot: Pilot Microsoft Edge and set up IE mode for the core group of stakeholders; use this opportunity to test IE mode and add any additional sites that require IE mode
Deploy: Microsoft Edge with IE mode to your organization after completing the pilot
Announce: Announce the move from Internet Explorer to Microsoft Edge to end users in your organization (End User Email 1)
Create buy-in: Generate excitement within

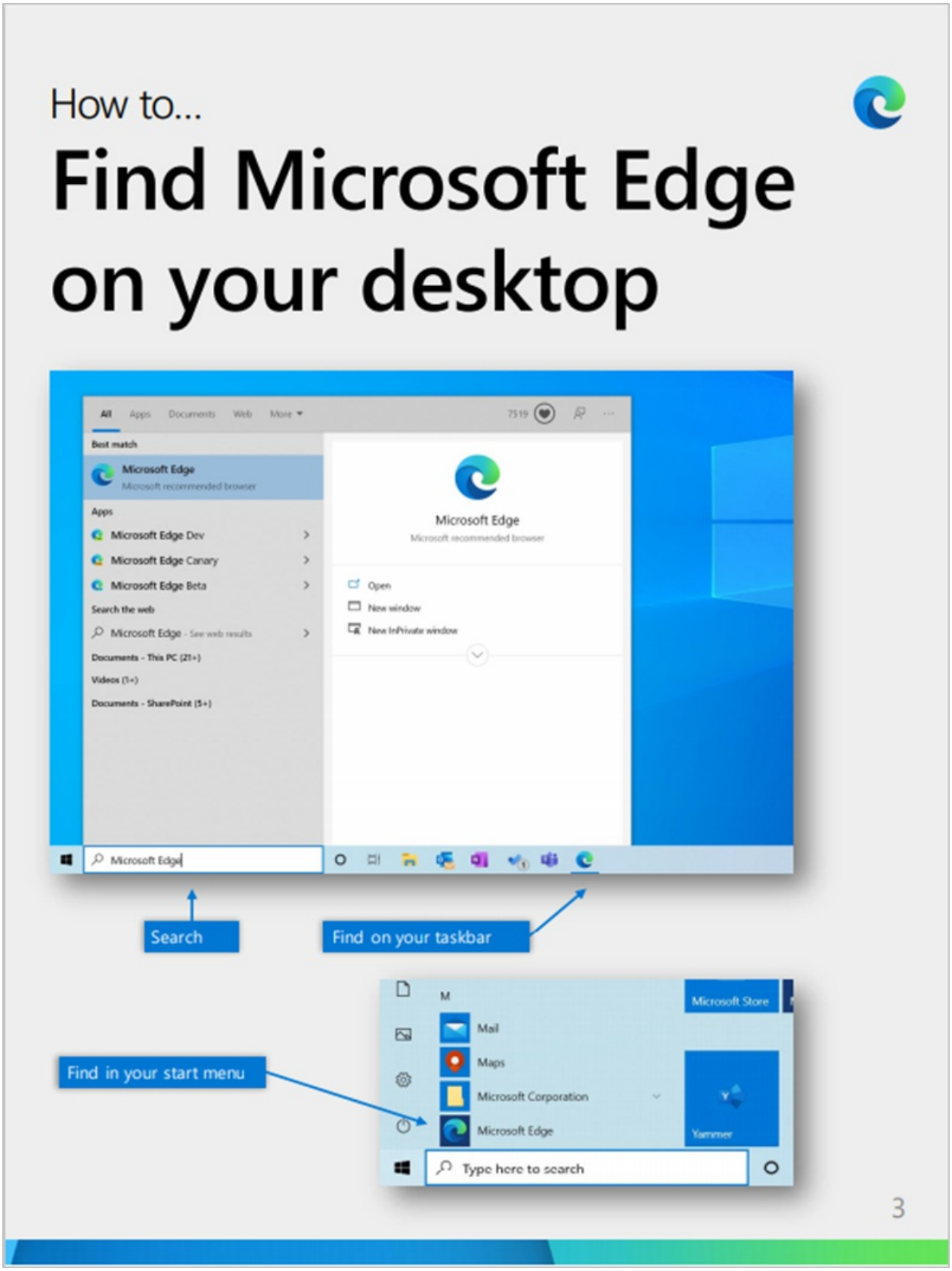
IT Deployment Guide

Use this guide to begin planning deployment and learn how to get started deploying Microsoft Edge in your environment.


Microsoft Mechanics video series
Learn how to deploy Microsoft Edge, set up Internet Explorer mode and configure with policies, and how to set up Microsoft Search with the Microsoft Edge playlist.
Deploy
Security & Compatibility
Microsoft Search
Microsoft Edge deployment
Options for your managed PCs, Macs and mobile devices
Microsoft Edge Management
Security, compatibility, and manageability of the new Microsoft Edge
Microsoft Search
Tailored search experience for information in your organization.
Get a hands-on tour of how to deploy Microsoft Edge to your devices.
Learn about Edge package options for automated installation, how to deploy Edge to Windows PCs using MECM (Microsoft Endpoint Configuration Manager), and steps to ensure all managed devices, including your phones and Macs, are provisioned with Edge.
Take a hands-on tour to experience the security, compatibility, and manageability of the new Microsoft Edge.
Edge is based on Chromium and designed to be the best browser for business. Our host, Jeremy Chapman, shows you what sets it apart from other browsers.
Get a hands-on tour of Microsoft Search, tailored experience to search for information in your organization.
You can easily find people, files, org charts, sites, and answers to common questions. See how it works, how to set it up quickly, and the advanced capabilities to help your users find the information they need to get work done.
Check out the playlist at https://aka.ms/EdgeforIT.
4
Microsoft

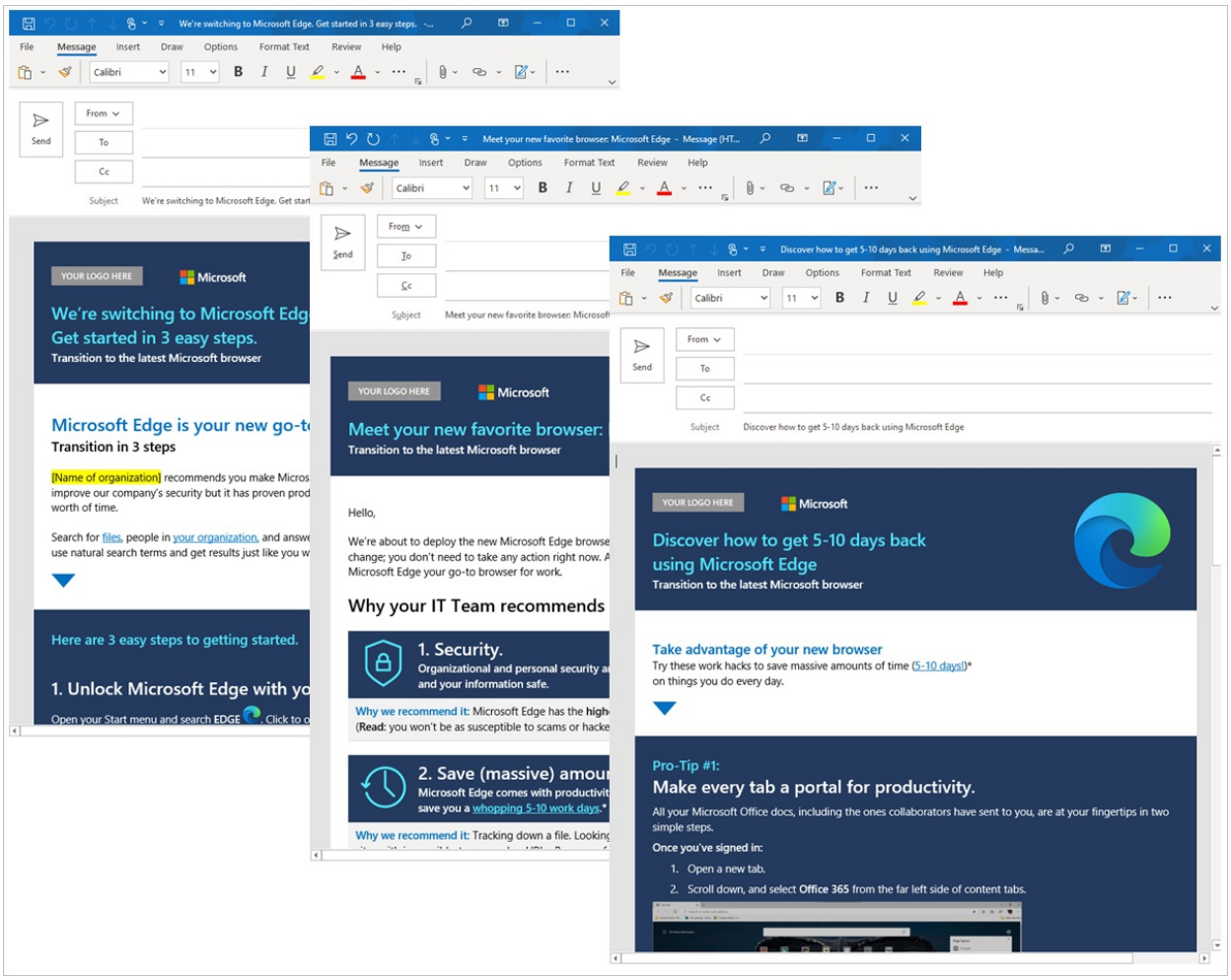
How to Get Started User Guide

Use this guide to educate users about Microsoft Edge. The guide includes overviews of the UI, menus, and features. We've also included tips to help users get started.



Adoption Email Templates

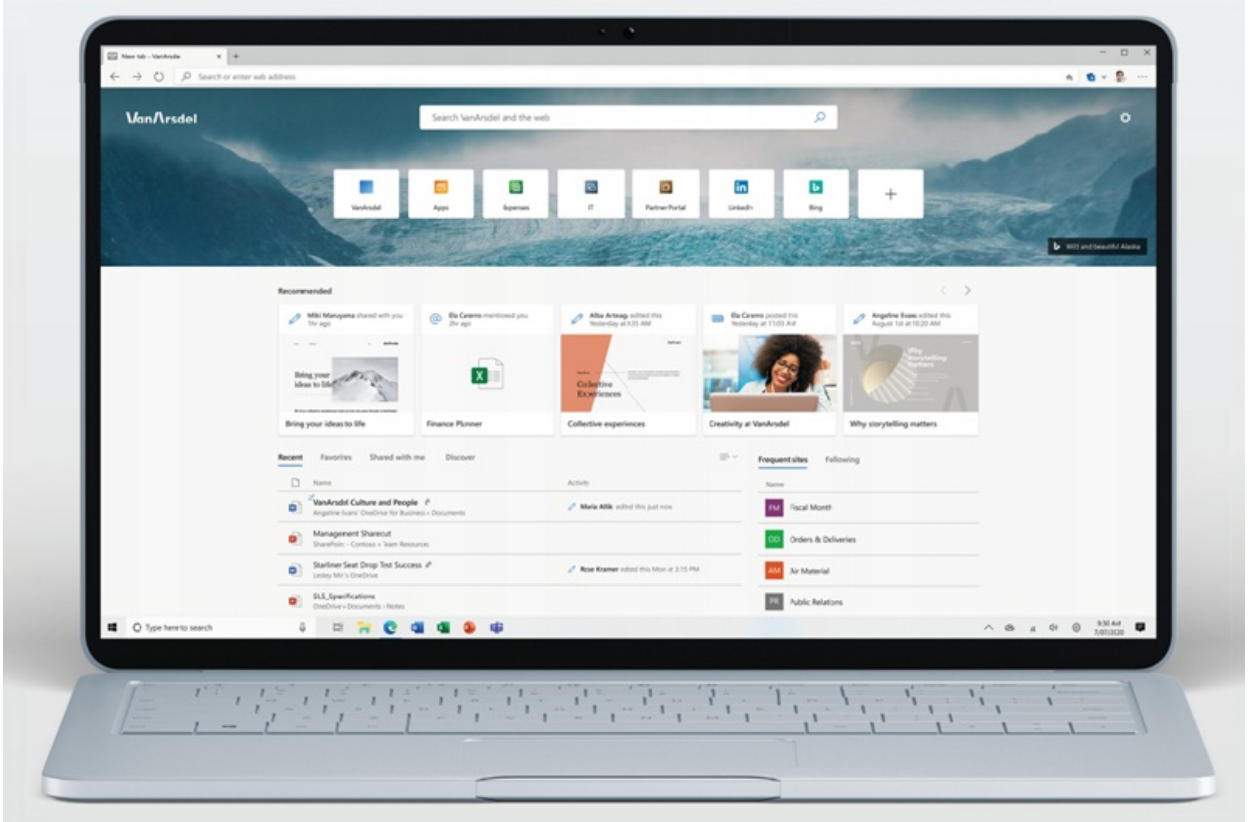
Use email to achieve a smooth transition as you rollout Microsoft Edge to end users. We've packaged a set of emails for you to use as an internal campaign. They provide tips and articulate how Microsoft Edge can save time and simplify their workday. The following screenshot shows an example of these templates.


We're switching to Microsoft Edge. Get started in 3 easy steps.
Meet your new favorite browser: Microsoft Edge - Message (HT...
Discover how to get 5-10 days back using Microsoft Edge - Messa...
YOUR LOGO HERE
Microsoft
We're switching to Microsoft Edg
Get started in 3 easy steps.
Transition to the latest Microsoft browser
Microsoft Edge is your new go-t
Transition in 3 steps
Here are 3 easy steps to getting started.
1. Unlock Microsoft Edge with yo
Meet your new favorite browser:
Transition to the latest Microsoft browser
Hello,
Why your IT Team recommends
1. Security.
2. Save (massive) amou
Discover how to get 5-10 days back using Microsoft Edge
Transition to the latest Microsoft browser
Take advantage of your new browser
Pro-Tip #1:
Make every tab a portal for productivity.
All your Microsoft Office docs, including the ones collaborators have sent to you, are at your fingertips in two simple steps.
Once you've signed in:
1. Open a new tab.
2. Scroll down, and select Office 365 from the far left side of content tabs.

Digital Signage

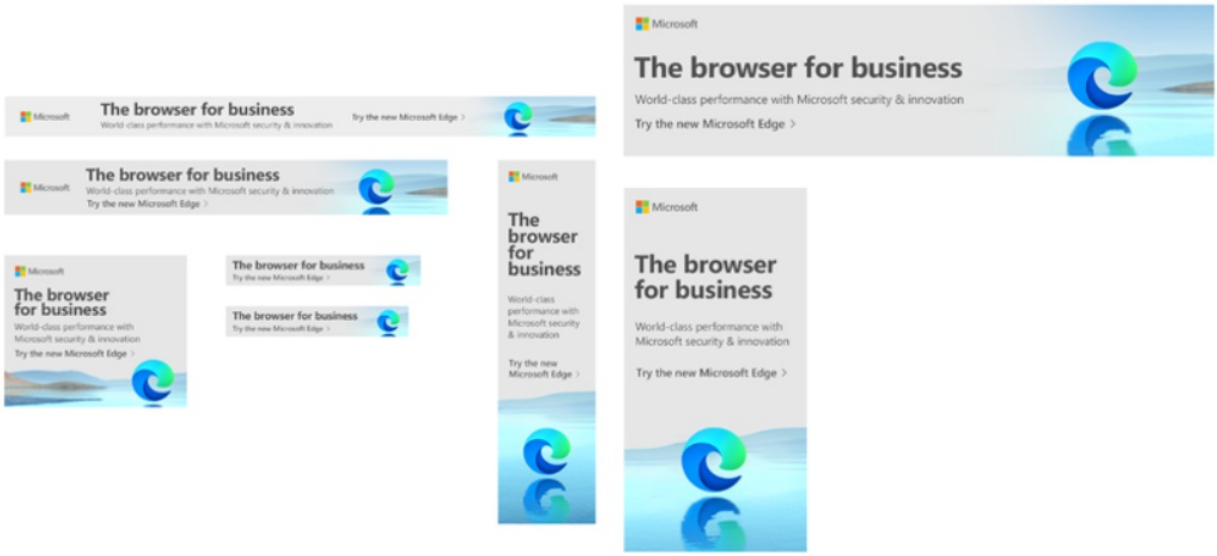
Use the following digital signage to inform users about Microsoft Edge:

- Enterprise new tab page
- Multiple Profiles and Cross Platform
- Microsoft Search in Bing
- Security



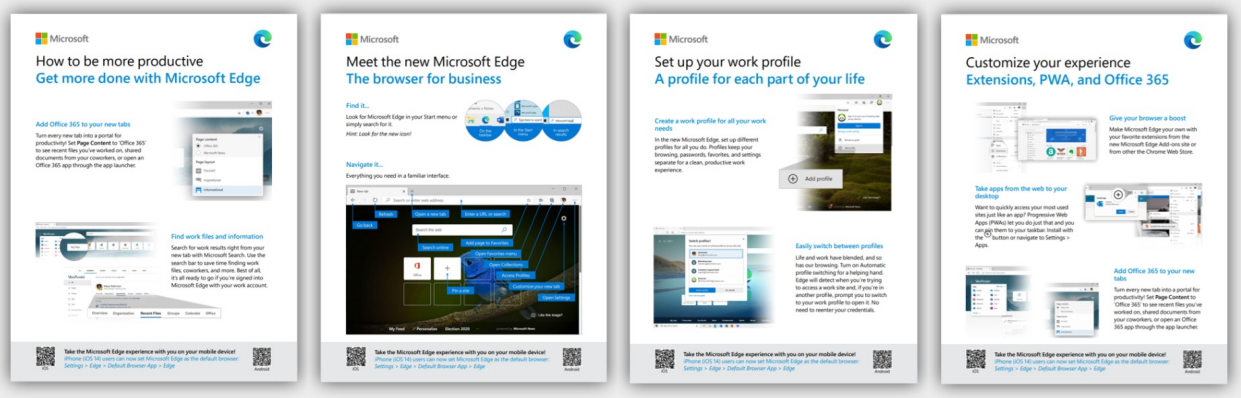
Banners

Use these banners on your internal sites to advertise Microsoft Edge to your employees.


Microsoft
The browser for business
World-class performance with Microsoft security & innovation
Try the new Microsoft Edge

One-pagers

Send or post these one-pagers to help your employees learn about Microsoft Edge and set up the browser for use at work.


Microsoft
How to be more productive
Get more done with Microsoft Edge
Add Office 365 to your new tabs
Find work files and information
Microsoft
Meet the new Microsoft Edge
The browser for business
Find it...
Navigate it...
Microsoft
Set up your work profile
A profile for each part of your life
Create a work profile for all your work needs
Add profile
Easily switch between profiles
Microsoft
Customize your experience
Extensions, PWA, and Office 365
Give your browser a boost
Take apps from the web to your desktop
Add Office 365 to your new tabs

Other learning resources

If you're interested in learning more about the benefits of Microsoft Edge, visit our webpage.

See also

- Microsoft Edge setup guide
- Microsoft Edge Enterprise landing page

Microsoft Edge hands-on deployment lab

11/1/2022 • 2 minutes to read • Edit Online

The Microsoft Edge team partnered with the Windows and Office Deployment Lab to create an area for you to test Microsoft Edge in a virtual environment. This lab automates the configuration of a virtual M365 desktop/management environment that lets you provision Microsoft Edge in a Microsoft Endpoint Configuration Manager instance.

About the lab guides

The step-by-step lab guides will take you through multiple deployment and management scenarios. These scenarios include the latest versions of Microsoft Intune and Configuration Manager (Version 1910). You'll see Microsoft Edge has been added to the Device and App Readiness section of the step-by-step labs.

For more information, see the Windows and Office Deployment Lab Kit.

See also

- Microsoft Edge Enterprise landing page

Microsoft Edge frequently asked questions

11/1/2022 • 2 minutes to read • Edit Online

This article contains frequently asked questions (FAQ) about Microsoft Edge in the enterprise.

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

How do I know which version of Microsoft Edge I have?

Select the ellipses icon (...) in the upper-right corner of Microsoft Edge, and then select **Settings**. Select **About Microsoft Edge** to see your version of Microsoft Edge.

What about Internet Explorer 11?

> **NOTE**
> The retired, out-of-support Internet Explorer 11 (IE11) desktop application will be permanently disabled on certain versions of Windows 10 as part of the February 2023 Windows security update ("B") release scheduled for February 14, 2023. Learn more
>
> We highly recommend setting up IE mode in Microsoft Edge and disabling IE11 prior to this date to ensure your organization does not experience business disruption. Learn how

Does Microsoft Edge support ActiveX controls or Browser Helper Objects like Silverlight or Java?

No. Microsoft Edge doesn't support ActiveX controls or Browser Help Objects (BHOs) like Silverlight or Java. However, if you're running web apps that use ActiveX controls, BHOs, or legacy document modes on Internet Explorer 11, you can configure them to run in IE mode on Microsoft Edge. For more information, see Configure IE mode on Microsoft Edge.

Will favorites be ported over from the current version of Microsoft Edge or will I have to re-add them?

Microsoft Edge supports import from existing installs of Microsoft Edge, Chrome, Internet Explorer, and Firefox (on Win10). The following settings are supported for importing: Bookmarks, History, Passwords, and Autofill (payments, addresses, and generic forms). You can choose to import either from the First-run Experience or from browser settings.

What's the difference between the Stable, Beta, Dev, and Canary channels/builds?

The Stable channel of Microsoft Edge is the most stable channel we offer with enterprise-focused features ready for you to pilot and evaluate across your organization. The Beta channel allows you to validate the next Stable release with a representative set of users. The Stable and Beta channels are updated approximately every four weeks. The Dev and Canary channels continue to update weekly and daily, respectively. Offline installers (MSIs

and PKG files) are available only for Stable, Beta, and Dev channels. For more information, see Overview of Microsoft Edge channels.

What kind of extension support do I have with Microsoft Edge?

Microsoft Edge supports extensions from Microsoft Edge Insider Addons and the Chrome Web Store.

Do you support Mobile Device Management (MDM) and Microsoft Intune?

Yes. Configuring Microsoft Edge on Windows 10 using Microsoft Intune and Mobile Device Management (MDM) is now supported. For more information, see Configure Microsoft Edge using Microsoft Intune and Configure Microsoft Edge using Mobile Device Management.

Does Windows Server Update Services (WSUS) support the initial deployment of Microsoft Edge?

Yes. There are packages in the Microsoft Update Catalog that can be used for the initial deployment of Microsoft Edge via WSUS. After initial deployment, automatic updates are configured by default. For more information, see Update in WSUS for the new Microsoft Edge for Windows 10, version 1809, 1903, 1909, and 2004: October 29, 2020.

Manual updates can be done through a configuration management tool, like ConfigMgr.

Are Initial Preferences supported?

Yes. For more information, see Configure Microsoft Edge using Initial Preferences settings for the first run

See also

- Microsoft Edge documentation landing page
- Microsoft Edge Enterprise landing page

Microsoft Edge Enterprise Roadmap

11/1/2022 • 2 minutes to read • Edit Online

This article describes the roadmap for Microsoft Edge Enterprise.

Roadmap

Microsoft Edge has been added to the M365 Roadmap. Over time, you'll see the Microsoft Edge roadmap fill with more features and you can filter by selecting Microsoft Edge from the Products section. We are working to continuously improve the experience and we welcome your feedback. Take a look at what we currently have planned for the upcoming Microsoft Edge releases.

Site compatibility changes

The web is constantly evolving to improve the user experience, security, and privacy. In some cases, changes are significant enough to impact the functionality of existing webpages.

Visit the Site compatibility-impacting changes coming to Microsoft Edge site to see the high-impact changes that the Microsoft Edge team is currently tracking. Check back often; the Microsoft Edge team updates this page as timelines solidify and new changes are announced.

See also

- Microsoft Edge Enterprise landing page

Platform support for Microsoft Edge features

11/1/2022 • 2 minutes to read • Edit Online

This article summarizes platform support for Microsoft Edge features.

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

Feature matrix for platforms

The following tables summarize feature support for the Windows and macOS platforms.

> **NOTE**
> Android and iOS are currently not represented in the support tables however we're continuing to work on this information and will update accordingly.

SECURITY FEATURES	WIN 10	WIN 8.1	WIN 7	MACOS	LINUX	URL
Azure Active Directory (Azure AD) Conditional Access	Yes	Yes	Yes	Yes	Yes	Azure AD Conditional Access
Microsoft Defender Application Guard	Yes (1890+)	No	No	No	No	Microsoft Defender Application Guard
Microsoft Defender SmartScreen	Yes	Yes	Yes	Yes	Yes	Microsoft Defender SmartScreen
Microsoft Endpoint DLP	Yes	No	No	No	No	Microsoft Endpoint DLP
Password Monitor	Yes	Yes	Yes	Yes	Yes	Password Monitor
Password Generator	Yes	Yes	Yes	Yes	Yes	Password Generator
Windows Information Protection (WIP)	Yes (1607+)	No	No	No	No	WIP

IDENTITY FEATURES	WIN 10	WIN 8.1	WIN 7	MACOS	LINUX	URL
Automatic Sign In (hybrid/AAD-J)	Yes	Yes	Yes	No	Yes	hybrid/AAD-J
Automatic Sign In (domain joined)	Yes	Yes	Yes	No	No	domain joined
Automatic Sign In (OS default account is MSA)	Yes (1709+)	No	No	No	No	MSA
Browser to Web Single Sign On (SSO)	Yes	Yes	Yes	Yes	Yes	Browser-Web SSO
Guided Switch/"Automatic Profile Switching"	Yes	Yes	Yes	Yes	Yes	Using multiple profiles at work and at home
Multiple Profiles	Yes	Yes	Yes	Yes	Yes	Using multiple profiles at work and at home
On-premises sync for Active Directory (AD)	Yes	Yes	Yes	No	No	On-premises sync for Active Directory (AD) users
Seamless SSO	Yes (1709+)	Yes	Yes	Yes	Yes	Seamless SSO
SSO with Primary Refresh Token (PRT)	Yes (1709+)	Yes	Yes	No	No	SSO with PRT
Windows Integrated Authentication (WIA)	Yes	Yes	Yes	Yes* (Policy Required)	No	WIA

ADDITIONAL FEATURES	WIN 10	WIN 8.1	WIN 7	MACOS	LINUX	URL
Collections	Yes	Yes	Yes	Yes	Yes	Collections

ADDITIONAL FEATURES	WIN 10	WIN 8.1	WIN 7	MACOS	LINUX	URL
Enterprise New Tab Page	Yes	Yes	Yes	Yes	Yes	New Tab Page
IE mode	Yes	Yes	Yes	No	No	IE mode
Kiosk Mode	Yes	No	No	No	No	Kiosk Mode
Microsoft Search in Bing	Yes	Yes	Yes	Yes	Yes	Intelligent Search in Bing
PDF Reader	Yes	Yes	Yes	Yes	Yes	PDF Reader
Shopping	Yes	Yes	Yes	Yes	Yes	Shopping
Sleeping Tabs	Yes	Yes	Yes	Yes	Yes	Feature overview Latest Blog Post Group Policies
Sync	Yes	Yes	Yes	Yes	Yes	Enterprise Sync
Version Rollback	Yes	Yes	Yes	No	No	Version rollback
Vertical Tabs	Yes	Yes	Yes	Yes	Yes	

See also

- Microsoft Edge Enterprise landing page

Plan your deployment of Microsoft Edge

11/1/2022 • 10 minutes to read • Edit Online

This article describes the recommended practices for deploying Microsoft Edge in an enterprise environment.

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

Article content

The following sections provide specific guidance for planning your Microsoft Edge deployment.

- Evaluate your existing browser environment and browser needs
- Make sure your Windows 10 devices are ready
- Determine your deployment methodology
  - Deploy to end users by role
  - Deploy to end users by site
- Do site discovery
  - If you've already deployed and configured the legacy version of Microsoft Edge
  - If you've configured Internet Explorer as your default browser
  - Analyze site discovery data
- Determine your channel strategy
  - Multiple devices and channels
- Define and configure policies
  - Define your update strategy and policies
- Do app compatibility testing
  - Internal line of business app testing
  - Third party app support
- Deploy Microsoft Edge to a pilot group
- Validate your deployment
- Broad deployment of Microsoft Edge
- See also

Evaluate your existing browser environment and browser needs

Take time to understand your current browser state and project vision to ensure that all project stakeholders are aligned and working towards the same result.

Start by defining your current state:

- Which browsers are currently deployed in your environment?
- Which browser is set as the default browser?
- Do you need to use Internet Explorer for some of your apps?
- Do you use an Enterprise Mode Site List to configure Internet Explorer today?
- What OS platforms are supported in your environment? (Windows 10, macOS, Windows 7, Windows Server, etc.)

- What management tools do you use for browser management?
- Who is responsible for browser configuration and management?
- What is your process for validating browser compatibility?

After you understand the current state, you can determine the desired goals for your browser deployment, taking into account the following:

- Do you want to set Microsoft Edge as your default browser?
- How will you configure Microsoft Edge?
- What features are critical to configure as part of your initial deployment?
- What is the process for addressing any identified compatibility or configuration issues?

You should also understand the **prerequisites** for features you're interested in, such as:

- Windows Defender Application Guard
- Internet Explorer mode
- Authentication and sync

With these answers in mind, you're ready to planning your Microsoft Edge deployment.

Make sure your Windows 10 devices are ready

The Edge Stable channel requires the Latest Cumulative Update (LCU) from October 2019 (or later). If you attempt to deploy to a Windows 10 device that has an older LCU, then the installation will fail. For more details about the minimum LCU that must be applied before deploying Edge, see Windows updates to support the next version of Microsoft Edge.

Determine your deployment methodology

After you know your desired end state, you're ready to start planning how to get there. The two main ways to deploy Microsoft Edge are by role, and by site.

Deploy to end users by role

If app compatibility is your main concern, and you don't have a firm grasp on which apps to test, you might want to consider deploying to end users by role. This enables each wave of a phased deployment to provide feedback and insights on apps that might need to have their configuration modified to address compatibility issues.

Deploy to end users by site

If bandwidth is your primary concern, you might want to consider doing application compatibility testing up front. After you finish testing, deploy to end users by site so you can leverage caching other software delivery optimizations.

Do site discovery

If you have a dependency on legacy web applications, and plan to use Internet Explorer mode (which most customers do), then you probably need to do some additional site discovery.

If you've already deployed and configured the legacy version of Microsoft Edge

If you've already configured your Enterprise Site List to work for the legacy version of Microsoft Edge, then your work is almost done! The one thing you may need to add are neutral sites.

Neutral sites are typically sites that provide Single Sign-On (SSO). If you navigate to a neutral site from Microsoft Edge, then you want to stay in Microsoft Edge to authenticate. If navigate to a neutral site in Internet Explorer mode, then you want to stay in Internet Explorer mode to authenticate.

Identify any SSO (or other neutral) sites that you use and add these to your Enterprise Site List.

If you've configured Internet Explorer as your default browser

If you're currently only using Internet Explorer, you might not know which sites have upgraded to modern web standards and which still require Internet Explorer. You want to find these sites and add them to the Enterprise Site List. This lets you use Internet Explorer mode only on the sites that need it.

> **TIP**
> Use the Enterprise Site Discovery tools to discover the sites that might need Internet Explorer mode. You can collect collect data on computers running Windows Internet Explorer 8 through Internet Explorer 11 on Windows 10, Windows 8.1, or Windows 7.

Analyze site discovery data

After you've collected site data, we recommend the following 4-step process to analyze the data:

1. Sort the data by domain, and then by URL.
2. Define the boundaries of an "app" to configure for Internet Explorer mode. You want to include all the sites and web controls that define the app. But you don't want to include any extra sites and controls by defining the app too broadly. Some sites may be as simple as "http://contoso.com/app1" while others may require you to define multiple sites and pages.
3. Test the app to verify that it doesn't work natively. Many sites will offer modern content when they detect a modern browser, and only offer legacy content when they detect Internet Explorer.
4. Add the app to your Enterprise Site list if it fails testing.

> **NOTE**
> As a best practice, group all of the sites that comprise an app. If the sites all need to be used to accomplish one task, and if they tend to be updated together, that is a good indication that they should be grouped. This way, when you upgrade an app, it's easier to remove the entire site from Internet Explorer mode and start using a modern browser for that app.

Determine your channel strategy

Microsoft Edge is released in multiple channels.

> **NOTE**
> You can install more than one channel on a device

The Stable Channel is what you will want to deploy to most devices. However, you should consider a deployment strategy that includes multiple devices and multiple channels.

Multiple devices and channels

We recommend having a representative subset of devices configured to use the Beta Channel. This lets you preview upcoming changes to the browser. You can see if these changes are going to affect your end users or apps.

You might also want to make the Dev Channel (or even the Canary Channel) available to some roles, such as web developers. Consider whether you would like to target some devices with more fluid and rapidly changing channels, or simply make these channels available for users to opt to install.

Because it's possible to install multiple channels on a device, you can mitigate the risk of testing for users who have opted to install a pre-release channel. For example, if you have a user who's using the Beta Channel, and there's a problem, they can switch to the Stable Channel and continue working. This unblocks them until the issue can be fixed.

> **NOTE**
> If the user enabled Sync, then their configuration will sync across channels, making it even easier to transition between channels.

Define and configure policies

After you've created your Enterprise Site List, we recommend identifying and configuring the policies that you intend to deploy with Microsoft Edge. This ensures that these policies are applied when you perform your testing.

First, consider the first-run experience you want your users to have. If you want to automatically import settings from the current browser, configure the policy for AutoImportAtFirstRun.

For security policies, we recommend starting with the Microsoft Edge Security Baseline. The Security Baseline can be applied using the Microsoft Security Baselines Blog or by using Microsoft Intune.

For other policies, we recommend reviewing the policy configurations for Microsoft Edge and Microsoft Edge Updates.

Define your update strategy and policies

You also want to determine how you want to do updates after you deploy Microsoft Edge:

- **Allow Microsoft Edge to update itself** (default). If you choose to allow automatic updates of Microsoft Edge, then Microsoft Edge will automatically update itself at the pace determined by the channel(s) you deployed.
- **Update Microsoft Edge at your own pace**. If you prefer to have explicit control over when updates are deployed, you can disable automatic updates and deploy it yourself (see the Update Policy reference.) After you disable automatic updates you can deploy updates for each channel using one of the following tools:
- Intune
- Configuration Manager
- the deployment tool of your choice.

Regardless of your update strategy, we recommend leveraging a ringed deployment strategy. With automatic updates, this means having a representative sample of users running the Beta Channel, to identify issues with what will become the Stable Channel. With manual updates, this might also include additional validation of a pilot group after a new Stable Channel build is released. This is followed by broad deployment.

> **NOTE**
> Microsoft Edge support will only apply to the most recent version of Microsoft Edge in each channel

Do app compatibility testing

Application compatibility for Microsoft Edge is extremely high - so high that Microsoft provides the following compatibility promises:

1. If it works on Microsoft Edge *version 45 and earlier*, it will work on Microsoft Edge *version 77 and later*.
2. If it works on Internet Explorer, it will work on Microsoft Edge in Internet Explorer mode.
3. If it works on Google Chrome, it will work on Microsoft Edge.

If you have an application where we don't meet our compatibility promise, then we stand behind the promise to fix it with Microsoft App Assure.

Internal line of business app testing

Despite our compatibility promise, we know that many organizations must validate some applications for their compliance or risk management reasons. Even though we expect this to be very straightforward, it's important to be organized and rigorous in app testing.

There are 2 ways to do app compatibility testing:

1. Lab testing. Applications are validated in a tightly controlled environment with specific configurations.
2. Pilot testing. Applications are validated by a limited number of users in their daily work environment using their own devices.

Choose the method that is most appropriate for each app, to manage risk without over-investing in compatibility testing.

Third party app support

In addition to their own line of business apps, many organizations use apps provided by external sources. The Ready for Microsoft Edge article contains a list of web applications that may be in use within your organization. This list provides links to provider support statements for their products when used with Microsoft Edge.

Deploy Microsoft Edge to a pilot group

After you've defined your policies and have finished your initial app compatibility testing, you're ready to deploy to your pilot group. Deploy to your pilot group using one of the following tools:

- Microsoft Intune for Windows, or Microsoft Intune for macOS
- Configuration Manager.
- Another management tool, download and deploy the MSI file for Microsoft Edge.

Validate your deployment

After you deploy your pilot, you want to capture all the feedback you get from your users.

- Capture feedback on compatibility. Identify sites that belong on the Enterprise Site List that weren't identified during site discovery.
- Capture feedback on the policy configuration. Ensure that users can use key features and do their work while following security guidelines.
- Capture feedback on ease of use and new features. Identify any areas where training should be developed and delivered based on user questions.

Broad deployment of Microsoft Edge

After a finishing the pilot and updating your deployment plan with lessons learned from the pilot, you're ready to do a full deployment of Microsoft Edge to all your users. Congratulations!

See also

- Microsoft Edge Enterprise landing page

- Video - Deploy Microsoft Edge

Microsoft Edge in your environment

11/1/2022 • 2 minutes to read • Edit Online

This article describes how to prepare to deploy Microsoft Edge when Microsoft Edge Legacy reaches its end of service.

As per the Microsoft Edge Product Team's blog post, support for the Microsoft Edge Legacy desktop application will end on March 9, 2021. When you apply the Update Tuesday (or "B") release in April, it will remove Microsoft Edge Legacy from devices running Windows 10 RS4 through 20H1 and replace it with Microsoft Edge.

How to Prepare

To prepare for Microsoft Edge being installed on Windows 10 RS4 through 20H1 devices with the Update Tuesday release in April, we recommend reading Plan your deployment of Microsoft Edge.

After you plan your deployment, use one of the following approaches to prepare to deploy Microsoft Edge.

- **Install group policies to customize your Microsoft Edge update approach**. For more information, see Configure Microsoft Edge policy settings on Windows, and pay special attention to the Update Policy reference material. If you install group policies to manage your updates before installing April's Update Tuesday release, Microsoft Edge will immediately start respecting your policy. If there isn't any installed group policy, Microsoft Edge will automatically update itself.
- **Remove the Microsoft Edge Legacy desktop application before its end of service date of March 9, 2021 and deploy Microsoft Edge**. For Windows 10 RS4 through 20H1, you can do this by using Windows Updates. For more information, see Deploy Microsoft Edge with Windows 10 updates.

See also

- Microsoft Edge Enterprise landing page
- Plan your deployment of Microsoft Edge

Microsoft browser usage report

11/1/2022 • 2 minutes to read • Edit Online

In the Microsoft 365 Admin Center, activity reports help you to see how users are using different Microsoft 365 services. See Activity Reports in the Microsoft 365 admin center.

Browser usage report

The Microsoft Browser Usage report in the Microsoft 365 Admin Center lets you see if users access Microsoft 365 online services via one of three Microsoft browsers: Internet Explorer 11, Microsoft Edge Legacy, or Microsoft Edge. With proper permissions, you can access the report on the usage dashboard and then see which browsers are used in your organization to access these online services. These report insights can help you migrate your organization to Microsoft Edge. To learn how access and use this report, see Microsoft 365 Reports in the admin center - Microsoft browser usage.

See also

- Microsoft Edge Enterprise landing page

Ready for Microsoft Edge

11/1/2022 • 3 minutes to read • Edit Online

The article provides information for the IT Administrator who's planning a Microsoft Edge deployment and needs information about application compatibility and support.

Web application compatibility and support

To help you plan your deployment of Microsoft Edge, we've compiled a list of web applications that may be in use within your organization. This list lets you determine if the web application is ready for Microsoft Edge, as documented by the web application provider's public support statement.

Add to the application list

The list is regularly updated as support statements are identified from customer engagement feedback.

If you are a web app provider and would like your support statement included for customer reference, please mail the following information to isvoutreach@microsoft.com.

- Product name
- Version Supported (if applicable)
- Provider Name
- Public Support Statement URL

Application list

Microsoft doesn't test or certify these applications in Microsoft Edge. The list was compiled based on publicly available resources. Always refer to the provider's current support statement. Some applications may require the use of IE Mode as indicated by the support statement.

The following table lists provider support statements for Microsoft Edge.

PROVIDER	PRODUCT	SUPPORT STATEMENT
Accruent	TMS 5.23	https://www.accruent.com/resources/blog-posts/accruent-enhances-tms-microsoft-edge-compatibility-new-automations?utm_source=linkedin&utm_medium=organic-social&utm_campaign=healthcare-general
Acumatica	Acumatica ERP	https://help-2020r1.acumatica.com/Wiki/(W(1))/ShowWiki.aspx?pageid=a8d5d39d-513a-4f93-b484-a95eb33103a1
Adaptive (Workday)	Workday Adaptive Planning	https://www.adaptiveplanning.com/uk/products/adaptive-technology-foundation
Adobe	Creative Cloud Products (Acrobat, Photoshop, Illustrator)	https://helpx.adobe.com/creative-cloud/system-requirements.html?promoid=P79NQR4R&mv=other

PROVIDER	PRODUCT	SUPPORT STATEMENT
Airtable	Airtable	https://support.airtable.com/hc/en-us/articles/217990018-What-are-the-technical-requirements-for-using-Airtable-
Alfresco Software	Alfresco Content Services	https://docs.alfresco.com/content-services/5.2/support/
Alteryx	Alteryx Analytics Platform	https://help.alteryx.com/current/product-activation-and-licensing/version-support-policy
Aprimo	Aprimo Cloud Marketing Studio	https://help.aprimo.com/Content/Marketing_Operations_Help/aprimo_basics/browsers_configuring_concept.html
Asana	Asana	https://asana.com/guide/help/faq/connectivity#gl-browsers
Atlassian	Bitbucket	https://confluence.atlassian.com/bitbucketserver/supported-platforms-776640981.html
Atlassian	OpsGenie	https://docs.opsgenie.com/docs/browser-compatibility
Atlassian	Confluence	https://confluence.atlassian.com/doc/supported-platforms-207488198.html
Atlassian	Jira	https://confluence.atlassian.com/adminjiraserver/supported-platforms-938846830.html
Atlassian	All other cloud products	https://confluence.atlassian.com/cloud/supported-browsers-744721663.html
Atlassian	Trello	https://help.trello.com/article/735-what-browsers-and-mobile-platforms-does-trello-support
Autodesk	AutoCAD Web	https://knowledge.autodesk.com/support/autocad-web-app/learn-explore/caas/CloudHelp/cloudhelp/ENU/AutoCAD-Web-Help/files/Settings-and-Preferences/AutoCAD-Web-Help-browsers-html-html.html
Bentley Systems	iTwin Services - Design Validation	https://communities.bentley.com/products/digital-twin-cloud-services/itwin-services/w/design-validation-wiki/43947/technical-requirements

PROVIDER	PRODUCT	SUPPORT STATEMENT
Box	Box	https://support.box.com/hc/en-us/articles/360052807333-Box-officially-supports-the-new-Microsoft-Edge-Browser
Cisco	WebRTC	https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingApps/WebRTC_important_info/Release_Notes_CMA_webRTC_latest.pdf
Cisco	WebEx	https://help.webex.com/en-us/nki3xrq/Webex-Meetings-Suite-System-Requirements#concept_6C8ED62012334D2D91D139BAD77C833F
Clarizen	Success	https://success.clarizen.com/hc/en-us/articles/205712188-Supported-Browsers?search=edge
Coda	Coda	https://help.coda.io/en/articles/1638088-which-browsers-does-coda-support
Cybozu	Kintone	https://jp.cybozu.help/general/en/user/list_start/webbrowser.html
Deltek	Vantagepoint Cloud	https://help.deltek.com/PRODUCT/Vantagepoint/2.0/CLOUDADMINGUIDE/Browser%20Interface.html
DocuSign	Docusign CLM	https://support.docusign.com/en/guides/SpringCM-Operating-System-and-Browser-Support
Doodle	Doodle	https://help.doodle.com/hc/en-us/articles/360012149773-What-are-the-system-requirements-for-using-Doodle-
DropBox	DropBox	https://help.dropbox.com/installs-integrations/desktop/system-requirements
Dynamic Signal	Dynamic Signal	https://support.dynamicsignal.com/hc/en-us/articles/360009309032-System-Requirements-and-Browser-Compatibility
Egnyte	Egnyte	https://helpdesk.egnyte.com/hc/en-us/articles/360030904532-Egnyte-Policy-for-Browser-and-OS-Support
Envoy	Envoy	https://envoy.help/en/articles/3449087-tls-compatibility

PROVIDER	PRODUCT	SUPPORT STATEMENT
Evernote	Web Clipper	https://help.evernote.com/hc/en-us/articles/208314738-Evernote-Web-Clipper-settings
Expensify.com	Expensify	https://community.expensify.com/categories/expensify-classroom
FreshBooks	FreshBooks	https://support.freshbooks.com/hc/en-us/articles/360003047891-Which-web-browsers-can-I-use-with-FreshBooks-
Freshworks	Freshdeck	https://support.freshdesk.com/support/solutions/articles/227719-system-and-browser-requirements-for-freshdesk
Gainsight	Gainsight	https://support.gainsight.com/PX/Install_PX/Browser_Compatibility_%2F%2F_Supported_Browser_List
GE	Predix Design System	https://www.ge.com/digital/documentation/predix-essentials/latest/supported-software-devices.html
Genesys	eServices, Administrator Extension, Pulse	https://docs.genesys.com/Documentation/System/Current/SOE/Welcome#t-1
GitLab	GitLab	https://docs.gitlab.com/ee/install/requirements.html
GoToMeeting (LogMeIn)	GoToMeeting (LogMeIn)	https://support.goto.com/meeting/help/system-requirements-for-organizers-g2m010024
Grammarly	Grammarly	https://support.grammarly.com/hc/en-us/articles/115000090811-What-do-I-need-in-order-to-use-Grammarly-
Greenhouse	Greenhouse Recruiting	https://support.greenhouse.io/hc/en-us/articles/360037604731-Greenhouse-Recruiting-Browser-Support
HCL	BigFix	https://help.hcltechsw.com/bigfix/9.5/platform/Platform/Installation/c_spcr_platform.html
Host Analytics	Host Analytics	https://help.hostanalytics.com/Release_Notes/2020_Release_Notes.htm?Highlight=release%20notes

PROVIDER	PRODUCT	SUPPORT STATEMENT
Host Analytics	CRM, CMS Hub, Marketing Hub, Sales Hub, Service Hub	https://knowledge.hubspot.com/resources/which-browsers-are-supported-by-hubspot
Hyland	ShareBase, OnBase	https://sharebase.onbase.com/en/faqs
Insightly	Insightly	https://support.insight.ly/hc/en-us/articles/204892624-Recommended-Browsers
Intercom	Intercom Messenger	https://www.intercom.com/help/en/articles/190-what-system-requirements-does-intercom-have
Intershop	Intershop	https://support.intershop.com/kb/index.php/Display/2929Y5
Intuit	Quickbooks	https://quickbooks.intuit.com/learn-support/global/help-articles/system-requirements-for-quickbooks-online/00/396218
Intuit	TurboTax	https://turbotax.intuit.com/personal-taxes/online/system-requirements
InVision	InVision	https://support.invisionapp.com/hc/en-us/articles/203009869-Which-browsers-and-design-tools-are-required-for-InVision-services-
Ivanti, Inc.	Workspace Control	https://forums.ivanti.com/s/article/INFO-Microsoft-Edge-Chromium-is-added-as-a-default-application-in-Websites-Security?language=en_US
Jaggaer	Jaggaer One	https://library.jaggaer.com/wp-content/uploads/Supported-Browsers-Devices.pdf
Laserfiche	Laserfiche	https://support.laserfiche.com/kb/1014127/laserfiche-compatibility-information-for-microsoft-edge-based-on-chromium
LexisNexis	LexisNexis	https://www.lexisnexis.com/en-us/gateway.page
Magneto Commerce	Magneto	https://devdocs.magento.com/guides/v2.4/install-gde/system-requirements.html
Marketo	Engage	https://docs.marketo.com/display/public/DOCS/Supported+Browsers

PROVIDER	PRODUCT	SUPPORT STATEMENT
MathWorks	MATLAB Online, Grader, Drive, ThingSpeak	https://www.mathworks.com/support/requirements/browser-requirements.html
Mavenlink	Mavenlink	https://mavenlink.zendesk.com/hc/en-us/articles/202489914-Mavenlink-Requirements
McAfee	Total Protection, LiveSafe, Internet Security, AntiVirus Plus, Small Business Security, Web Advisor	https://www.mcafee.com/en-us/consumer-support/help/system-requirement.html
McAfee	DLPe 11.6	https://kc.mcafee.com/corporate/index?page=content&id=KB91647
Miro	Miro Realtime Board	https://help.miro.com/hc/en-us/articles/360017572814-Supported-Browsers
Monday.com	Monday	https://support.monday.com/hc/en-us/articles/360002145219-Supported-Web-Browsers
NetSuite (Oracle)	Oracle NetSuite	https://nlcorp.app.netsuite.com/core/media/media.nl?id=94209463&c=NLCORP&h=3735c785dc0db0151a4e&_xt=.pdf
New Relic	New Relic UI	https://docs.newrelic.com/docs/using-new-relic/user-interface-functions/view-your-data/supported-browsers-new-relics-ui
onepointProject	One Point Projects	http://ftp.onepoint-projects.com/documentation/latest/onepoint-server-installation.pdf
Pega	Pega CRM	https://community.pega.com/knowledgebase/articles/pega-platform-client-operating-system-and-browser-support
PeopleFluent	PeopleFluent Talent Management	https://tmhelp.peoplefluent.com/11.12.0.2.65509/en_US/End%20User/welcome.htm#t=common%2Fhw_sw_reqs%2Fweb_browser_support_policy.htm
Planview	PPM Pro	https://success.planview.com/Planview_PPM_Pro/150_PPM_Pro_Administrator_Documentation/015_System_Settings/004_System_Requirements
Qlik	QlikView Desktop	https://help.qlik.com/en-US/qlikview/April2019/Content/QV_HelpSites/System-requirements.htm

PROVIDER	PRODUCT	SUPPORT STATEMENT
Salesforce	Salesforce Classic, Einstein, Analytics Lightning Experience	https://resources.docs.salesforce.com/224/latest/en-us/sfdc/pdf/salesforce_spring20_release_notes.pdf
Sansan	Eight	https://eight.zendesk.com/hc/en-us/articles/360000571836-Recommended-environment-for-using-Eight
Sansan	Eight (JP)	https://eight.zendesk.com/hc/ja/articles/360000571836
SAS	SAS	https://support.sas.com/en/documentation/third-party-software-reference/9-4/support-for-9-4-web-browsers.html
Shopify	Shopify	https://help.shopify.com/en/manual/intro-to-shopify/shopify-admin/supported-browsers
Sitecore	Sirecore XP	https://kb.sitecore.net/articles/087164
Smartsheet	Smartsheet	https://help.smartsheet.com/articles/506775-system-requirements-for-using-smartsheet
Stack Overflow	Stack Overflow	https://stackoverflow.com/help/browser-support
SugarCRM	Shopify	https://support.sugarcrm.com/Resources/Supported_Platforms/
SumTotal	SumTotal Talent Expansion Suite	https://hr.ucmerced.edu/files/page/documents/browser_settings_-_sumtotal_compatibility_requirements.pdf
SurveyMonkey	SurveyMonkey	https://help.surveymonkey.com/articles/en_US/kb/What-browser-versions-do-you-support
Tableau	Tableau Server	https://www.tableau.com/products/techspecs#server
Tableau	Tableau Online	https://www.tableau.com/products/techspecs#online
Teleopti	Teleopti WFM Cloud	https://www.teleopti.com/archive/files/66907/service-specification_nov_21_2019-pdf.aspx service-specification

PROVIDER	PRODUCT	SUPPORT STATEMENT
TIBCO	Tibco Cloud Spotfire	https://docs.tibco.com/pub/spotfire/general/sr/GUID-12C6E934-C84C-499B-9DAC-DD510854E4E1.html
Verint	Verint Community	https://community.telligent.com/community/11/w/user-documentation/63073/what-are-the-system-requirements
Visma	Visma UX, Nordic Cool 4	https://ux.visma.com/weblibrary/latest/
Wrike	Wrike	https://help.wrike.com/hc/en-us/articles/115003289725-Supported-Browsers
Yesware	Yesware for Outlook	https://help.yesware.com/hc/en-us/articles/360046287974-What-browsers-and-operating-systems-does-Yesware-support-
Younglimwon	K-System Ace	https://www.ksystem.co.kr/k-system-ace/
Zapier	Zapier	https://zapier.com/help/troubleshoot/behavior/browsers-supported-by-zapier
Zendesk	Zendesk Support	https://support.zendesk.com/hc/en-us/articles/203661786-Zendesk-Support-system-requirements
Zendesk	Zendesk Helpcenter	https://support.zendesk.com/hc/en-us/articles/115001505447
Zendesk	Zendesk Chat	https://support.zendesk.com/hc/en-us/articles/360022362053-Zendesk-Chat-system-requirements
Zendesk	Zendesk Sell	https://support.zendesk.com/hc/en-us/articles/360041515433-Zendesk-Sell-system-requirements-
Zipwhip	Zipwhip	https://support.zipwhip.com/s/article/Supported-Web-Browsers-and-Operating-Systems
Zoho	One, CRM	https://www.zoho.com/projects/help/kbase/accounts-faq.html
Zoom	Zoom	https://support.zoom.us/hc/en-us/articles/201362023-System-Requirements-for-PC-Mac-and-Linux#h_92957a85-2506-43a2-bd4a-5bb274778518

PROVIDER	PRODUCT	SUPPORT STATEMENT
ZScaler	Zscaler	https://help.zscaler.com/zia/supported-browsers

See also

- Microsoft Edge Enterprise landing page
- Plan your deployment of Microsoft Edge

Release notes for Microsoft Edge Mobile Stable Channel

11/1/2022 • 2 minutes to read • Edit Online

These release notes provide information about new features that are available to work or school accounts, and non-security updates that are included in the Microsoft Edge for Mobile Stable Channel.

To understand Microsoft Edge channels, see the Overview of the Microsoft Edge channels.

All the Stable channel security updates are listed in Release notes for Microsoft Edge Security Updates.

> **NOTE**
> For the Stable Channel, updates roll out progressively over one or more days. To learn more, see Progressive rollouts for Microsoft Edge updates. There might be a delay before the new release is populated to the App Store (iOS) and Google Play (Android).

Version 106.0.1370.47: October 17, 2022

Fixed various bugs and performance issues.

Version 105.0.1343.38: September 13, 2022

Fixed various bugs.

Version 104.0.1293.60: August 17, 2022

> **IMPORTANT**
> This update contains a fix for CVE-2022-2856, which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here.

Version 104.0.1293.58: August 16

Fixed various bugs.

Feature updates

- **Support for disabling of inPrivate browsing and Password feature (iOS and Android).** Before Microsoft Edge 104, Edge for iOS and Android disabled InPrivate browsing and Password (prompts to save passwords for the user) by default when only allow Work or School Accounts is configured.

  Starting with Microsoft Edge 104, you have more flexibility because InPrivate and Password won't be disabled by default when only allow Work or School Accounts is configured. Instead, you can decide whether to disable InPrivate browsing or Password by configuring the **com.microsoft.intune.mam.managedbrowser.disabledFeatures** key. For more information, see Disable specific features.

Version 103.1264.53: July 1

Fixed various bugs.

Version 103.0.1264.38: June 30

Fixed various bugs.

Version 102.0.1245.30: May 31

Fixed various bugs.

Feature updates

- **Support switching network stack between Chromium and iOS (iOS only).** The NetworkStackPref policy lets you choose the network preference for Microsoft Edge for iOS.

Policy updates

New policies

- NetworkStackPref - Choose the network preference for Microsoft Edge for iOS

Version 101.0.1210.43: May 9

Fixed various bugs.

Version 101.0.1210.32: April 29

Fixed various bugs.

Feature updates

- **Read Aloud: background play and play in silent mode (iOS and Android)**
  - When playing in the background, users can control Read Aloud (pause, resume, play forwards, or play backwards) via the notification panel and lock screen.
  - When a user switches tabs in Microsoft Edge while using Read Aloud, they can use a floating control bar to pause, resume, or close Read Aloud.
  - When a device's silent toggle is on, it doesn't affect Read Aloud playback as long as media volume is turned up.

See also

- Microsoft Edge Enterprise landing page

Release notes for Microsoft Edge Stable Channel

11/1/2022 • 6 minutes to read • Edit Online

These release notes provide information about new features and non-security updates that are included in the Microsoft Edge Stable Channel.

- All the security updates are listed in Release notes for Microsoft Edge Security Updates.
- Archived release notes for Microsoft Edge Stable Channel are located in Archived release notes for Microsoft Edge Stable Channel.

To understand Microsoft Edge channels, see the Overview of the Microsoft Edge channels.

> **NOTE**
>
> For the Stable Channel, updates will roll out progressively over one or more days. To learn more, see Progressive rollouts for Microsoft Edge updates.
>
> Microsoft Edge Web Platform constantly evolves to improve user experience, security, and privacy. To learn more, see Site compatibility-impacting changes coming to Microsoft Edge.

Version 107.0.1418.26: October 29, 2022

> **IMPORTANT**
>
> This update contains a fix for CVE-2022-3723, which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here.

Version 106.0.1370.61: October 29, 2022

> **IMPORTANT**
>
> This update to Extended Stable contains a fix for CVE-2022-3723, which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here

Version 106.0.1370.59: October 27, 2022

Fixed various bugs and performance issues for Extended Stable release.

Version 107.0.1418.24: October 27, 2022

Stable channel security updates are listed here.

Feature updates

- **Microsoft Edge sidebar.** The Microsoft Edge sidebar lets users access productivity tools side-by-side with their browsing window. For enterprise customers, the following experiences are currently turned on

by default: Search, Discover, Office.com, and Outlook. Administrators can control the availability and configure the Microsoft Edge sidebar using the HubsSidebarEnabled, ExtensionInstallBlockList, and ExtensionInstallForceList policies. The extension ID for each sidebar app can be found at *edge://sidebar-internals*. For more information, see Manage the sidebar in Microsoft Edge.

- **New policy to give more flexibility in Microsoft Edge startup.** The RestoreOnStartupUserURLsEnabled policy lets users add and remove their own URLs to open when starting Microsoft Edge while maintaining the mandatory list of sites specified by the admin.

Policy updates

New policies

- EdgeWorkspacesEnabled - Enable Workspaces
- EnhanceSecurityModeBypassIntranet - Enhanced Security Mode configuraton for Intranet zone sites
- EventPathEnabled - Re-enable the Event.path API until Microsoft Edge version 115
- InternetExplorerIntegrationLocalMhtFileAllowed - Allow local MHTML files to open automatically in Internet Explorer mode
- LinkedAccountEnabled - Enable the linked account feature
- PerformanceDetectorEnabled - Performance Detector Enabled
- RestoreOnStartupUserURLsEnabled - Allow users to add and remove their own sites during startup when the RestoreOnStartupURLs policy is configured
- DefaultShareAdditionalOSRegionSetting - Set the default "share additional operating system region" setting
- WebSelectEnabled - Web Select Enabled
- WebSQLAccess - Force WebSQL to be enabled
- WebSQLNonSecureContextEnabled - Force WebSQL in non-secure contexts to be enabled

Deprecated policy

- MicrosoftOfficeMenuEnabled - Allow users to access the Microsoft Office menu

Obsoleted policy

- BuiltinCertificateVerifierEnabled - Determines whether the built-in certificate verifier will be used to verify server certificates

Version 106.0.1370.52: October 20, 2022

Fixed various bugs and performance issues for Stable and Extended Stable release.

Version 106.0.1370.47: October 14, 2022

Stable channel security updates are listed here.

Version 106.0.1370.42: October 10, 2022

Fixed various bugs and performance issues.

Version 106.0.1370.37: October 6, 2022

Fixed various bugs and performance issues.

Version 106.0.1370.34: October 3, 2022

Stable channel security updates are listed here.

Feature updates

- **More reliable web defense.** Browse the web with more reliable protection thanks to the rewritten

Microsoft Defender SmartScreen library for Microsoft Edge on Windows and macOS. The new SmartScreen library was first made available on Windows with Microsoft Edge version 103, and now makes its debut on macOS with Microsoft Edge version 106. The NewSmartScreenLibraryEnabled policy is now deprecated in Microsoft Edge version 106 and will be obsolete in Microsoft Edge version 108.

- **Increased Work Results in the Microsoft Edge address bar.** We've increased the maximum number of work results that display in the address bar from 2 to 4, which offers greater visibility into the work content available to you as you search. This feature requires the AddressBarMicrosoftSearchInBingProviderEnabled policy enabled to work.

Policy updates

New policies

- EfficiencyModeEnabled - Efficiency mode enabled
- EfficiencyModeOnPowerEnabled - Enable efficiency mode when the device is connected to a power source
- InternetExplorerIntegrationAlwaysUseOSCapture - Always use the OS capture engine to avoid issues with capturing Internet Explorer mode tabs

Deprecated policies

- NewSmartScreenLibraryEnabled - Enable new SmartScreen library
- ShadowStackCrashRollbackBehavior - Configure ShadowStack crash rollback behavior

Obsoleted policies

- OutlookHubMenuEnabled - Allow users to access the Outlook menu
- EdgeDiscoverEnabled - Discover feature In Microsoft Edge

Version 105.0.1343.53: September 26, 2022

Fixed various bugs and performance issues.

Version 105.0.1343.50: September 22, 2022

Fixed various bugs and performance issues.

Version 105.0.1343.42: September 15, 2022

Stable channel security updates are listed here.

Version 104.0.1293.91: September 15, 2022

Fixed various bugs and performance issues for Extended Stable release.

Version 105.0.1343.33: September 8, 2022

Fixed various bugs and performance issues.

Version 104.0.1293.81: September 2, 2022

> **IMPORTANT**
> This update to Extended Stable contains a fix for CVE-2022-3075, which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here

Version 105.0.1343.27: September 2, 2022

> **IMPORTANT**
>
> This update contains a fix for CVE-2022-3075, which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here.

Version 105.0.1343.25: September 1, 2022

Stable channel security updates are listed here.

Feature updates

- **Enhanced security mode improvements.** Enhanced security mode now supports WebAssembly for x64 Windows. Additional cross-platform support is expected in the future. For more information, see Browse more safely with Microsoft Edge.
- **Improvement to the Cloud Site List Management experience for IE mode.**
  - You can restore to one of the last 3 published versions of your site list in the Microsoft 365 Admin Center. For more information, see Restore a previous version of a site list.
  - You can identify gaps in your enterprise site list by configuring reporting of site feedback with the InternetExplorerIntegrationCloudUserSitesReporting and InternetExplorerIntegrationCloudNeutralSitesReporting policies. You can view local site list URLs from users and potentially misconfigured neutral site URLs in the Microsoft Edge site lists experience in the Microsoft 365 Admin Center. To learn more, see View site feedback on the Microsoft 365 Admin Center.
  - You can configure session cookie sharing between Microsoft Edge and Internet Explorer for IE mode on your site list in the Microsoft 365 Admin Center. To learn more, see Cookie sharing between Microsoft Edge and Internet Explorer.
- **Improvements to the Cloud Site List Management experience for IE mode now available in GCC.** GCC customers can now utilize the full Microsoft Edge site list experience in the Microsoft 365 Admin Center.

Policy updates

New policies

- ExemptFileTypeDownloadWarnings - Disable download file type extension-based warnings for specified file types on domains
- InternetExplorerIntegrationAlwaysWaitForUnload - Wait for Internet Explorer mode tabs to completely unload before ending the browser session
- MicrosoftEditorProofingEnabled - Spell checking provided by Microsoft Editor
- MicrosoftEditorSynonymsEnabled - Synonyms are provided when using Microsoft Editor spell checker
- PrintPdfAsImageDefault - Print PDF as Image Default
- UnthrottledNestedTimeoutEnabled - JavaScript setTimeout will not be clamped until a higher nesting threshold is set

Deprecated policies

- ExemptDomainFileTypePairsFromFileTypeDownloadWarnings - Disable download file type extension-based warnings for specified file types on domains

Additional policy changes

- GuidedSwitchEnabled - Add Linux platform support

Version 104.0.1293.78: September 1, 2022

Fixed various bugs and performance issues for Extended Stable release.

Version 104.0.1293.70: August 25, 2022

Fixed various bugs and performance issues.

See also

- Microsoft Edge Enterprise landing page

Archived release notes for Microsoft Edge Stable Channel

11/1/2022 • 91 minutes to read • Edit Online

These release notes provide information about new features and non-security updates that are included in the Microsoft Edge Stable Channel. All the security updates are listed here.

Version 104.0.1293.63: August 19

> **IMPORTANT**
>
> This update contains a fix for CVE-2022-2856, which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here.

Feature updates

- **Search in the Microsoft Edge sidebar.** Easily access an updated sidebar search via Microsoft Edge sidebar, including easy access to Microsoft Search in Bing for organizations. Note: This is a controlled feature rollout. If you don't see this feature, check back as we continue our rollout.
- **Gaming for the Microsoft Edge sidebar.** Play popular casual games for free. Administrators can control the availability of the Games menu in the Microsoft Edge sidebar. Note: This is a controlled feature rollout. If you don't see this feature, check back as we continue our rollout.
- **Discover in the Microsoft Edge sidebar.** Discover content relevant to the page you're browsing including summaries, source information, and more. Note: This is a controlled feature rollout. If you don't see this feature, check back as we continue our rollout.
- **Get your favorite tools in the Microsoft Edge sidebar.** Easily access commonly used tools while you browse the web, including Calculator, Internet speed test, and Unit converter. Note: This is a controlled feature rollout. If you don't see this feature, check back as we continue our rollout.
- **Outlook in the Microsoft Edge sidebar.** Quickly and easily access Outlook Mail and Calendar. Note: This is a controlled feature rollout. If you don't see this feature, check back as we continue our rollout.
- **Office in the Microsoft Edge sidebar.** Quickly and easily access Microsoft Office documents and apps. Administrators can control the Microsoft Office menu in the Microsoft Edge sidebar. Note: This is a controlled feature rollout. If you don't see this feature, check back as we continue our rollout.

Version 104.0.1293.54: August 11

Fixed various bugs and performance issues for Stable and Extended Stable release.

Version 104.0.1293.47: August 5

Stable channel security updates are listed here.

Feature updates

- **Enhance your security on the web**. Improvements to **Enhance your security on the web** in

edge://settings/privacy now include **Basic** as the new default option. With this option, Microsoft Edge will apply added security protection to the less visited sites. This feature preserves the user experience for the most popular sites on the web. For more information, see Browse more safely with Microsoft Edge.

- **Import Chrome data without Chrome during First Run Experience.** This feature lets a user bring in their Chrome data by logging in to their Google account during Microsoft Edge's First Run Experience. This feature can be turned off by disabling First Run Experience with the HideFirstRunExperience policy, or by setting AutoImportAtFirstRun to 'DisabledAutoImport'.

Policy updates

New policies

- AllowedDomainsForApps - Define domains allowed to access Google Workspace
- AskBeforeCloseEnabled - Get user confirmation before closing a browser window with multiple tabs
- BrowserCodeIntegritySetting - Configure browser process code integrity guard setting
- DoubleClickCloseTabEnabled - Double Click feature in Microsoft Edge enabled (only available in China)
- ImportOnEachLaunch - Allow import of data from other browsers on each Microsoft Edge launch
- QuickSearchShowMiniMenu - Enables Microsoft Edge mini menu
- PasswordManagerRestrictLengthEnabled - Restrict the length of passwords that can be saved in the Password Manager
- PDFXFAEnabled - XFA support in native PDF reader enabled
- TextPredictionEnabled - Text prediction enabled by default

Obsoleted policy

- U2fSecurityKeyApiEnabled - Allow using the deprecated U2F Security Key API

Version 103.0.1264.77: July 28

Fixed various bugs and performance issues.

Version 102.0.1245.62: July 27

Fixed various bugs and performance issues for Extended Stable release.

Version 103.0.1264.71: July 22

Stable channel security updates are listed here.

Version 103.0.1264.62: July 14

Fixed various bugs and performance issues. We recommend that users install this update to address the following issue.

Known issue

Microsoft Edge on 32-bit (x86) Windows 10 Version 1809 may experience startup issues with the upcoming July Non-Security Windows Updates (KB5015880 - 17763.3224). This is fixed with the latest Microsoft Edge Stable channel release, version 103.0.1264.62. Enterprise users encountering this issue on Microsoft Edge Extended Stable channel version 102 need to disable the NewSmartScreenLibraryEnabled policy.

Version 103.0.1264.49: July 6

IMPORTANT

This update contains a fix for CVE-2022-2294, which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here.

Version 102.0.1245.56: July 6

Fixed various bugs and performance issues for Extended Stable release.

Version 103.0.1264.44: June 30

Stable channel security updates are listed here.

Version 102.0.1245.50: June 23

Fixed various bugs and performance issues for Extended Stable release.

Version 103.0.1264.37: June 23

Stable channel security updates are listed here.

Feature updates

- **Ability to control automatic profile switching.** The GuidedSwitchEnabled policy lets Microsoft Edge prompt the user to switch to the appropriate profile when Microsoft Edge detects that a link is a personal or work link.
- **Client Certificate Switcher.** This feature will offer a way for users to clear the remembered certificate and resurface the certificate picker when visiting a site requiring http certificate authentication. Switching can be done without manually quitting Microsoft Edge.
- **More reliable web defense.** Browse the web with more reliable protection thanks to the rewritten Microsoft Defender SmartScreen library for Microsoft Edge on Windows. The NewSmartScreenLibraryEnabled policy will allow enterprise customers to continue using the legacy version of the library until it's deprecated in Microsoft Edge version 105.
- **Work Search Banner in the Microsoft Edge address bar.** This banner helps you stay in the flow of your work by narrowing your search focus to work-only results. To see work focused results from your organization, select the banner at the beginning of your search. To be directed to your organization's workplace search results page, select the banner at any point of your search. Use the AddressBarMicrosoftSearchInBingProviderEnabled policy to turn this feature on or off.

Policy updates

New policies

- GuidedSwitchEnabled - Guided Switch Enabled
- InternetExplorerZoomDisplay - Display zoom in IE Mode tabs with DPI Scale included like it is in Internet Explorer
- LiveCaptionsAllowed - Live captions allowed
- OriginAgentClusterDefaultEnabled - Origin-keyed agent clustering enabled by default

Additional policy changes

- SleepingTabsTimeout - Set the background tab inactivity timeout for sleeping tabs. **Note:** A timeout of 30 seconds of inactivity was added to this policy.

Version 102.0.1245.44: June 16

Fixed various bugs and performance issues for Stable and Extended Stable release.

Version 102.0.1245.41: June 13

Stable channel security updates are listed here.

Version 102.0.1245.39: June 9

Stable channel security updates are listed here.

Version 102.0.1245.33: June 3

Fixed various bugs and performance issues for Stable and Extended Stable release.

Version 102.0.1245.30: May 31, 2022

Stable channel security updates are listed here.

Policy updates

New policies

- AllHttpAuthSchemesAllowedForOrigins - List of origins that allow all HTTP authentication
- OutlookHubMenuEnabled - Allow users to access the Outlook menu
- NetworkServiceSandboxEnabled - Enable the network service sandbox
- UserAgentClientHintsGREASEUpdateEnabled - Control the User-Agent Client Hints GREASE Update feature

Version 101.0.1210.53: May 19, 2022

Fixed various bugs and performance issues.

Version 100.0.1185.60: May 13, 2022

Fixed various bugs and performance issues for Extended Stable release.

Version 101.0.1210.47: May 13, 2022

Stable channel security updates are listed here.

Version 101.0.1210.39: May 5, 2022

Fixed various bugs and performance issues.

Version 100.0.1185.57: May 2, 2022

Fixed various bugs and performance issues for Extended Stable release.

Version 101.0.1210.32: April 28

Stable channel security updates are listed here.

Feature updates

- **Ability to set the default profile.** The EdgeDefaultProfileEnabled policy will let you set a default profile to use when opening the browser instead of the last profile that was used. This policy won't be

applicable if the `--profile-directory` parameter has been specified.

- **Launch Progressive Web Apps (PWAs) from the favorites bar.** Improvements to the PWA launch experience will start appearing with an Apps icon that can be added to the toolbar.
- **Manage the "Allow extensions from other stores" setting.** Now you can use the ControlDefaultStateOfAllowExtensionFromOtherStoresSettingEnabled policy to set the default state of the "Allow extensions from other stores" setting.
- **Improvements to the Enterprise Site List Manager.** Now you can configure shared cookies between Microsoft Edge and Internet Explorer on your enterprise site list. You can access the Enterprise Site List Manager at *edge://compat/SiteListManager*.

Policy updates

New policies

- ConfigureKeyboardShortcuts - Configure the list of commands for which to disable keyboard shortcuts
- ControlDefaultStateOfAllowExtensionFromOtherStoresSettingEnabled - Configure default state of Allow extensions from other stores setting
- EdgeAssetDeliveryServiceEnabled - Allow features to download assets from the Asset Delivery Service
- EdgeDefaultProfileEnabled - Default Profile Setting Enabled
- InternetExplorerModeEnableSavePageAs - Allow Save page as in Internet Explorer mode
- KioskSwipeGesturesEnabled - Swipe gestures in Microsoft Edge kiosk mode enabled
- MicrosoftOfficeMenuEnabled - Allow users to access the Microsoft Office menu
- SiteSafetyServicesEnabled - Allow users to configure Site safety services

Deprecated policies

- ForceCertificatePromptsOnMultipleMatches - Configure whether Microsoft Edge should automatically select a certificate when there are multiple certificate matches for a site configured with "AutoSelectCertificateForUrls"

Obsoleted policies

- WebSQLInThirdPartyContextEnabled - Force WebSQL in third-party contexts to be re-enabled

Version 100.0.1185.50: April 21

Fixed various bugs and performance issues for Stable and Extended Stable release.

Version 100.0.1185.44: April 15

> **IMPORTANT**
> This update contains a fix for CVE-2022-1364, which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here.

Version 100.0.1185.39: April 11

Fixed various bugs and performance issues for Stable and Extended Stable release.

Version 100.0.1185.36: April 7

Stable channel security updates are listed here.

Version 100.0.1185.29: April 1

Stable channel security updates are listed here.

Feature updates

- **Three-digit version number in the User-agent string.** Microsoft Edge will now send a three-digit version number, such as Edg/100 in the User-Agent header. This may confuse scripts or server-side analytics that use a buggy parser to determine the User-Agent string version number. You can use the ForceMajorVersionToMinorPositionInUserAgent policy to control whether the User-Agent string major version should be frozen at 99. Also, the **#force-major-version-to-minor** flag is available in *edge://flags* to freeze the major version in the User-Agent string to 99.

- **Streamlining Microsoft 365 Application Protocol Activations.** Microsoft 365 Application Protocol Activations on trusted Microsoft cloud storage services will now launch certain Microsoft 365 applications directly, including SharePoint subdomains and Microsoft OneDrive URLs. You can use the policies AutoLaunchProtocolsComponentEnabled and AutoLaunchProtocolsFromOrigins to enable the application protocol activation prompts if desired, and to define other applications and services where warnings are enabled or disabled.

- **Hardware-enforced Stack Protection.** Microsoft Edge will continue supporting more fine-grained protection by combating memory corruption vulnerabilities and by protecting indirect calls. Hardware-enforced stack protection is only supported by Windows 8 and later. For more information, see Hardware-enforced Stack Protection. This feature behavior can be controlled using the ShadowStackCrashRollbackBehavior policy.

- **Preview PDF files in Microsoft Outlook and File Explorer.** Users can view a PDF file in a lightweight and rich read-onlypreview. This feature is available for Outlook Desktop PDF attachments or for local PDF files using File Explorer.

- **Open Digitally Signed PDF files.** Digital signatures are used extensively to validate the authenticity of a document and changes made in a document. You can use the PDFSecureMode policy to enable digital signature validation for PDF files, directly from the browser, without the need for any add-ins.

Policy updates

New policies

- AdsTransparencyEnabled - Configure if the ads transparency feature is enabled
- DefaultWebHidGuardSetting - Control use of the WebHID API
- HideRestoreDialogEnabled - Hide restore pages dialog after browser crash
- PDFSecureMode - Secure mode and Certificate-based Digital Signature validation in native PDF reader
- PromptOnMultipleMatchingCertificates - Prompt the user to select a certificate when multiple certificates match
- WebHidAskForUrls - Allow the WebHID API on these sites
- WebHidBlockedForUrls - Block the WebHID API on these sites

Deprecated policy

- BackgroundTemplateListUpdatesEnabled - Enables background updates to the list of available templates for Collections and other features that use templates

Obsoleted policy

- AllowSyncXHRInPageDismissal - Allow pages to send synchronous XHR requests during page dismissal

Version 98.0.1108.92: March 26

Fixed various bugs and performance issues for Extended Stable release.

Version 99.0.1150.55: March 26

> **IMPORTANT**
> This update contains a fix for CVE-2022-1096, which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here.

Version 99.0.1150.52: March 24

Fixed various bugs and performance issues.

Version 98.0.1108.84: March 17

Fixed various bugs and performance issues for Extended Stable release.

Version 99.0.1150.46: March 17

Stable channel security updates are listed here.

Version 99.0.1150.39: March 10

Fixed various bugs and performance issues.

Version 98.0.1108.76: March 9

Fixed various bugs and performance issues for Extended Stable release.

Version 99.0.1150.36: March 7

Fixed various bugs and performance issues.

Version 99.0.1150.30: March 3

Stable channel security updates are listed here.

Feature updates

- **Upcoming three-digit version number in user agent string.** Starting with version 100, Microsoft Edge will send a three-digit version number in the User-Agent header, for example "Edg/100". Starting with Microsoft Edge 97, site owners can test this upcoming agent string by enabling the **#force-major-version-to-100** experiment flag in *edge://flags* to ensure their User-Agent parsing logic is robust and works as expected.
- **Personalize multi-profile experiences with profile preferences for sites.** Users can personalize their multi-profile experience with the ability to create a customized list of sites for automatic profile switching in Microsoft Edge.
- **Navigate PDF documents using page thumbnails.** You'll now be able to navigate through your PDF document using thumbnails that represent the pages. These thumbnails will appear in the pane on the left side of the PDF reader.
- **Configure the list of domains for which the password manager User Interface (UI) for Save and Fill will be disabled.** Use the PasswordManagerBlocklist policy to configure the list of domains (HTTP/HTTPS schemas and hostnames only) where Microsoft Edge should disable the password manager.

This means that Save and Fill workflows will be disabled, which ensures that passwords for those websites can't be saved or auto filled into web forms.

- **Custom primary password.** The browser already has the capability where users can add an authentication step before saved passwords are auto filled in web forms. This adds another layer of privacy and helps prevent unauthorized users from using saved passwords to log on websites. Custom primary password is an evolution of that same feature, where users will now be able to use a custom string of their choice as their primary password. After it's enabled, users will enter this password to authenticate themselves and have their saved passwords auto filled into web forms.

Policy updates

New Policies

- DoNotSilentlyBlockProtocolsFromOrigins - Define a list of protocols that can not be silently blocked by anti-flood protection
- ForceMajorVersionToMinorPositionInUserAgent - Enable or disable freezing the User-Agent string at major version 99
- HubsSidebarEnabled - Show Hubs Sidebar
- InternetExplorerIntegrationCloudNeutralSitesReporting - Configure reporting of potentially misconfigured neutral site URLs to the M365 Admin Center Site Lists app
- InternetExplorerIntegrationCloudUserSitesReporting - Configure reporting of IE Mode user list entries to the M365 Admin Center Site Lists app
- PasswordManagerBlocklist - Configure the list of domains for which the password manager UI (Save and Fill) will be disabled
- RelatedMatchesCloudServiceEnabled - Configure Related Matches in Find on Page
- SignInCtaOnNtpEnabled - Enable sign in click to action dialog
- UserAgentReduction - Enable or disable the User-Agent Reduction

Version 98.0.1108.62: February 24

Fixed various bugs and performance issues for Stable and Extended Stable release.

Version 98.0.1108.56: February 17

Fixed various bugs and performance issues for Stable and Extended Stable release.

Version 98.0.1108.55: February 16

> **IMPORTANT**
>
> This update contains a fix for CVE-2022-0609, which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here.

Version 98.0.1108.50: February 10

Stable channel security updates are listed here.

Version 98.0.1108.43: February 3

Stable channel security updates are listed here.

Feature updates

- **Enhance your security on the web.** This is a browsing mode in Microsoft Edge where browser security takes priority, giving users an extra layer of protection when browsing the web. Administrators can apply group policies to end-user desktops (Windows, macOS, and Linux) to help protect against in-the-wild exploits (also referred to 0-days). The following group policies support this browsing mode:
  - EnhanceSecurityMode
  - EnhanceSecurityModeBypassListDomains
  - EnhanceSecurityModeEnforceListDomains
- **Upcoming three-digit version number in user agent string.** Starting with version 100, Microsoft Edge will send a three-digit version number in the User-Agent header, for example "Edg/**100**". Starting with Microsoft Edge 97, site owners can test this upcoming user agent string by enabling the **#force-major-version-to-100** experiment flag in *edge://flags* to ensure their User-Agent parsing logic is robust and works as expected.
- **Deprecate WebRTC's Plan B SDP semantics.** This change deprecates a legacy Session Description Protocol (SDP) dialect called Plan B. This SDP format is being replaced by the Unified Plan, which is a spec-compliant and cross-browser compatible SDP format. For more information, see the Chrome Platform Status entry PSA: Plan B should throw in M96 Beta and Stable, and PSA: Plan B throwing in Stable and Extended Deprecation Trial End Date. Requesting a Trial for RTCPeerConnection Plan B SDP Semantics allows sites to continue to use the deprecated API until version 101.
- **Overlay scrollbars added to Microsoft Edge.** We've updated our scrollbars with an overlay-based design. Users can turn this feature on in *edge://flags*.

Policy updates

New Policies

- AddressBarEditingEnabled - Configure address bar editing
- AllowGamesMenu - Allow users to access the games menu
- EdgeFollowEnabled - Enable Follow service in Microsoft Edge
- EnhanceSecurityMode - Enhance the security state in Microsoft Edge
- EnhanceSecurityModeBypassListDomains - Configure the list of domains for which enhance security mode will not be enforced
- EnhanceSecurityModeEnforceListDomains - Configure the list of domains for which enhance security mode will always be enforced
- InAppSupportEnabled - In-app support Enabled
- MicrosoftEdgeInsiderPromotionEnabled - Microsoft Edge Insider Promotion Enabled
- PrintStickySettings - Print preview sticky settings
- SandboxExternalProtocolBlocked - Allow Microsoft Edge to block navigations to external protocols in a sandboxed iframe
- U2fSecurityKeyApiEnabled - Allow using the deprecated U2F Security Key API

Version 97.0.1072.76: January 27

Fixed various bugs and performance issues.

Feature updates

- **Upcoming three-digit version number in user agent string.** Starting with version 100, Microsoft Edge will send a three-digit version number in the User-Agent header, for example "Edg/**100**". Starting with Microsoft Edge 97, site owners can test this upcoming user agent string by enabling the **#force-major-version-to-100** experiment flag in *edge://flags* to ensure their User-Agent parsing logic is robust and works as expected.

Version 96.0.1054.75: January 21

Fixed various bugs and performance issues for Extended Stable release.

Version 97.0.1072.69: January 20

Stable channel security updates are listed here.

Version 97.0.1072.62: January 13

Fixed various bugs and performance issues.

Version 96.0.1054.72: January 6

Fixed various bugs and performance issues for Extended Stable release.

Version 97.0.1072.55: January 6

Stable channel security updates are listed here.

Feature updates

- **Use the current profile to sign into websites when multiple work or school accounts are signed in on a device.** When multiple work or school accounts are signed in on a device, users will be asked to choose an account from the account picker to continue their visits to websites. In this release, users will be prompted to let Microsoft Edge sign in to the websites automatically with the work or school account that's signed into the current profile. Users can turn this feature on and off in **Settings** > **Profile preferences**.
- **Add support for Microsoft Endpoint Data Loss Prevention (DLP) on macOS.** Microsoft Endpoint DLP policy enforcement will be available natively on macOS.
- **Automatic HTTPS.** Users can upgrade navigations from HTTP to HTTPS on domains likely to support this more secure protocol. This support can also be configured to attempt delivery over HTTPS for all domains. Note: This feature is a Controlled Feature Rollout. If you don't see this feature, check back as we continue our rollout.
- **Block WebSQL in 3rd-party contexts.** Use of the legacy WebSQL feature will be blocked from 3rd-party frames. The WebSQLInThirdPartyContextEnabled policy is available as an opt-out option until Microsoft Edge version 101. This change is happening in the Chromium project that Microsoft Edge is based on. For more information, see this Chrome Platform Status entry.
- **Citations in Microsoft Edge.** Citing sources for research is a common requirement for students. They have to manage many research references and sources, which aren't easy tasks. They also have to translate these citations to proper citation formats like APA, MLA, and Chicago. This new "Citations" feature, now in Preview in Microsoft Edge, gives students a better way to manage and generate citations as they research online. With Citations turned on in Collections or from **Settings and more (Alt-F)**, Microsoft Edge automatically generates citations that students can use later so they can stay focused on their research. When they're done, they can easily compile these citations into a final deliverable. For more information, see Previewing Citations in Microsoft Edge.
- **Control Flow Guard (CFG).** Microsoft Edge will start supporting more fine-grained protection by combating memory corruption vulnerabilities and by protecting indirect calls. CFG is only supported with Windows 8 and later. For more information, see Control Flow Guard.

> **NOTE**
> This is an evolving technology, please share your feedback to help us strengthen its support.

Policy updates

New Policies

- AccessibilityImageLabelsEnabled - Get Image Descriptions from Microsoft Enabled
- CORSNonWildcardRequestHeadersSupport - CORS non-wildcard request header support enabled
- EdgeDiscoverEnabled - Discover feature In Microsoft Edge
- EdgeEnhanceImagesEnabled - Enhance images enabled
- InternetExplorerModeTabInEdgeModeAllowed - Allow sites configured for Internet Explorer mode to open in Microsoft Edge
- SameOriginTabCaptureAllowedByOrigins - Allow Same Origin Tab capture by these origins
- ScreenCaptureAllowedByOrigins - Allow Desktop, Window, and Tab capture by these origins
- SerialAllowAllPortsForUrls - Automatically grant sites permission to connect all serial ports
- SerialAllowUsbDevicesForUrls - Automatically grant sites permission to connect to USB serial devices
- SmartScreenDnsRequestsEnabled - Enable Microsoft Defender SmartScreen DNS requests
- TabCaptureAllowedByOrigins - Allow Tab capture by these origins
- WebSQLInThirdPartyContextEnabled - Force WebSQL in third-party contexts to be re-enabled
- WindowCaptureAllowedByOrigins - Allow Window and Tab capture by these origins

Version 96.0.1054.62: December 17

Fixed various bugs and performance issues.

Version 96.0.1054.57: December 14

> **IMPORTANT**
> This update contains a fix for CVE-2021-4102, which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here.

Version 96.0.1054.53: December 10

Stable channel security updates are listed here.

Version 96.0.1054.43: December 2

Fixed various bugs and performance issues.

Version 96.0.1054.41: November 30

Fixed various bugs and performance issues.

Version 96.0.1054.34: November 23

Fixed various bugs and performance issues.

Version 96.0.1054.29: November 19

Stable channel security updates are listed here.

Feature updates

- **Cloud Site List Management for IE mode in Public Preview.** Cloud Site List Management lets you manage your site lists for IE mode in the cloud without needing an on-premises infrastructure to host your organization's site list. You can access the Cloud Site List Management feature using the Microsoft Edge Site Lists experience in the Microsoft 365 Admin Center. To learn more, see the Cloud Site List Management for IE mode (Public Preview) article.
- **Improved handoff between IE mode and the modern browser.** Starting with this version of Microsoft Edge, navigations between Microsoft Edge and Internet Explorer mode will include form data and additional HTTP headers. Referrer headers, post data, forms data, and request methods will be forwarded correctly across the two experiences. You can specify which data types should be included using the InternetExplorerIntegrationComplexNavDataTypes policy. For more information, see this FAQ: My application requires transferring POST data between IE mode and Microsoft Edge. Is this supported?
- **Update Microsoft Edge WebView2 using WSUS.** IT Admins using Windows Server Update Services (WSUS) to update Microsoft Edge will also be able to update Microsoft Edge WebView2 using WSUS. This capability gives admins an easier servicing process for offline devices.
- **WSUS updates for Server.** WSUS and Catalog updates for Microsoft Edge channels (Stable, Beta, and Dev) will now apply to Windows Server SKUs that have Microsoft Edge installed, including Windows Server 2022. For more information on how to configure WSUS updates for Microsoft Edge, see Update Microsoft Edge.
- **Microsoft Edge AutoLaunch Protocols Component.** Microsoft Edge 96 introduces the AutoLaunch Protocols Component that contains lists of scheme-origin dictionaries to automatically allow or block. This protects customers from dangerous schemes (for example, a protocol handler with a 0-day) while eliminating prompts from known-safe pairings (for example, the Teams website can open the Teams client app). If for some reason, you don't want Microsoft Edge to block vulnerable protocol handlers and allow known-safe pairings, use the toggle in *edge://settings/content/applicationLinks*, or set the AutoLaunchProtocolsComponentEnabled policy to False.
- **Launch Progressive Web App (PWA) directly via protocol links.** Let installed PWAs handle links that use a specific protocol for a more integrated experience.
- **Quickly view Office files in the browser.** Users can now view Office files including documents, spreadsheets, and presentations that they come across while browsing on Microsoft Edge right in the browser without needing to download the file and then open it in a different application. There will be no changes in the file open experience for Office files that are hosted on OneDrive or SharePoint.
- **Freeform highlighting on PDFs.** The PDF viewing and markup experience is improved with the addition of freeform highlighters. You can highlight sections in PDFs that you don't have access to, and scanned documents.
- **Hardware-enforced Stack Protection.** Microsoft Edge will begin supporting an even safer browsing mode that uses hardware-dependent control flow for browser processes on supported hardware (Intel 11th Gen. or AMD Zen 3). Note: Because this is a Controlled Feature Rollout you may not notice this feature enabled on all devices. You can enable or disable Hardware-enforced Stack Protection by manipulating Image File Execution Options (IFEO) using group policy.
- **New warning dialog for typosquatting sites.** The browser will show a warning on some sites with URLs that look very similar to other sites. This UI uses client-side heuristics to warn users about sites that might be spoofing popular web sites. For more information, see What is typosquatting?.

- **Dictionary added to mini-toolbar in Immersive Reader.** We're adding dictionary functionality to the mini-toolbar to assist in your reading and research. You'll be able to look up the spelling and definitions of words more quickly and easily in the Immersive Reader experience.
- **Learn how to solve math problems with Math Solver.** We're excited to announce that you can use Math Solver in Microsoft Edge to get help with a wide range of mathematical concepts. These concepts range from elementary arithmetic and quadratic equations to trigonometry and calculus. Math Solver lets you take a picture of a handwritten or printed math problem and then provides an instant solution with step-by-step instructions to help you learn how to reach the solution without help. Math Solver also comes with a mathematical keyboard that you can use to easily type math problems. This keyboard eliminates the need to search around a traditional keyboard to find the math characters you need. After solving your problem, Math Solver provides options to continue learning with quizzes, worksheets, and video tutorials.
- **Split tunnel VPN support for WebRTC.** Allows enterprise customers to gain the benefit of VPN split tunneling for peer-to-peer traffic on Microsoft Edge. You can enable this feature using the WebRtcRespectOsRoutingTableEnabled policy.

Policy updates

New Policies

- ApplicationGuardUploadBlockingEnabled - Prevents files from being uploaded while in Application Guard
- AudioProcessHighPriorityEnabled - Allow the audio process to run with priority above normal on Windows
- AutoLaunchProtocolsComponentEnabled - AutoLaunch Protocols Component Enabled
- EfficiencyMode - Configure when efficiency mode should become active
- ForceSyncTypes - Configure the list of types that are included for synchronization
- InternetExplorerIntegrationComplexNavDataTypes - Configure whether form data and HTTP headers will be sent when entering or exiting Internet Explorer mode
- InternetExplorerModeToolbarButtonEnabled - Show the Reload in Internet Explorer mode button in the toolbar
- PrintPostScriptMode - Print PostScript Mode
- PrintRasterizePdfDpi - Print Rasterize PDF DPI
- RendererAppContainerEnabled - Enable renderer in app container
- SharedLinksEnabled - Show links shared from Microsoft 365 apps in History
- TyposquattingCheckerEnabled - Configure Edge TyposquattingChecker

Version 95.0.1020.53: November 12

Fixed various bugs and performance issues.

Version 95.0.1020.44: November 4

Fixed various bugs and performance issues.

Version 94.0.992.58: October 30

Fixed various bugs and performance issues for Extended Stable release.

Version 95.0.1020.40: October 29

IMPORTANT

This update contains a fix for CVE-2021-38000 and CVE-2021-38003 which have been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide

Stable channel security updates are listed here.

Version 95.0.1020.38: October 28

Fixed various bugs and performance issues.

Version 94.0.992.57: October 27

Fixed various bugs and performance issues for Extended Stable release.

Version 95.0.1020.30: October 21

Stable channel security updates are listed here.

Feature updates

- **View in File Explorer support for SharePoint Online libraries in Microsoft Edge.** Now you can enable the View in File Explorer capability on SharePoint Online Modern Document Libraries. For this experience to be visible and work for your users, you need to enable the Microsoft Edge policy Configure the View in File Explorer feature for SharePoint pages in Microsoft Edge and update your SharePoint Online tenant configuration. Learn more: View SharePoint files with File Explorer in Microsoft Edge.
- **Intranet zone file URL links will open in Windows File Explorer.** You can allow file URL links to intranet zone files originating from intranet zone HTTPS websites to open Windows File Explorer for that file or directory. You can enable this experience using the IntranetFileLinksEnabled policy.
- **Improvements to the downloads experience.** Support for the download user experience is extended to progressive web applications PWAs and WebView. We will also begin to support drag and drop to the File Explorer and Desktop.
- **Pick up where you left off on PDF documents.** You will now be able to resume reading from where you last closed your PDF document.
- **Efficiency mode extends battery life when your laptop enters battery saver mode.** Efficiency mode will become active when your laptop enters battery saver mode to allow the browser to manage resource usage to extend the battery life of your machine. You will have four options when efficiency mode becomes active: Unplugged and low battery, Unplugged, Always, and Never. Note: This feature is a Controlled Feature Rollout. If you don't see this feature, check back shortly as we continue our rollout.
- **Free form text boxes added to PDF documents.** We now support adding free form text boxes to PDF documents. You can use these boxes to fill in forms and add visible notes.
- **Citation support added to Collections.** We've improved the Collections experience, especially for students and researchers. Collections will start supporting citations and reading lists.
- **Update your passwords faster and with fewer clicks.** The browser will now take you directly to the Change Password page for a given website. This action saves you time and clicks by removing the need to navigate to the page manually. After you're on this page, the browser will also autofill your existing password and suggest a strong, unique new password. Note: Currently this feature is only available on a limited number of sites.
- **Auto-account creation.** We now provide additional support on Sign-Up pages by allowing you to

create an online account with one click. You can do this by selecting the suggestion drop-down when you click on any form field in the Sign-Up form. Doing so will show not only information relevant to the Sign-Up form, but also a strong new password suggestion. Upon selection, all the relevant information gets populated in the respective fields and the suggested password will be automatically stored on submission to the website. Note: Currently this feature is only available on a limited number of sites.

Policy updates

New Policies

- BrowserLegacyExtensionPointsBlockingEnabled Enable browser legacy extension point blocking
- CrossOriginWebAssemblyModuleSharingEnabled Specifies whether WebAssembly modules can be sent cross-origin
- DisplayCapturePermissionsPolicyEnabled Specifies whether the display-capture permissions-policy is checked or skipped
- InternetExplorerIntegrationWindowOpenHeightAdjustment Configure the pixel adjustment between window.open heights sourced from IE mode pages vs. Edge mode pages
- InternetExplorerIntegrationWindowOpenWidthAdjustment Configure the pixel adjustment between window.open widths sourced from IE mode pages vs. Edge mode pages
- IntranetFileLinksEnabled Allow intranet zone file URL links from Microsoft Edge to open in Windows File Explorer
- NewSmartScreenLibraryEnabled Enable new SmartScreen library
- ShadowStackCrashRollbackBehavior Configure ShadowStack crash rollback behavior
- VisualSearchEnabled Visual search enabled

Obsoleted Policies

- InternetExplorerIntegrationTestingAllowed Allow Internet Explorer mode testing
- LegacySameSiteCookieBehaviorEnabled Enable default legacy SameSite cookie behavior setting

Version 94.0.992.50: October 14

Fixed various bugs and performance issues.

Version 94.0.992.47: October 11

Stable channel security updates are listed here.

Version 94.0.992.38: October 1

> **IMPORTANT**
> This update contains a fix for CVE-2021-37975 and CVE-2021-37976 which have been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide

Stable channel security updates are listed here.

Version 94.0.992.37: September 30

Fixed various bugs & performance issues.

Version 94.0.992.31: September 24

IMPORTANT

This update contains a fix for CVE-2021-37973 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here.

Feature updates

- **Microsoft Edge has completed the move to a 4-week cadence for updates.** We have adopted a new 4-week release cycle for major versions. Read more here: https://blogs.windows.com/msedgedev/2021/03/12/new-release-cycles-microsoft-edge-extended-stable/
- **New Extended stable option being offered.** We are offering a new Extended Stable option to our managed Enterprise customers. The Extended Stable option will stay on even numbered revisions and update every 8 weeks. There will be a biweekly security update. Additional information here: https://blogs.windows.com/msedgedev/2021/07/15/opt-in-extended-stable-release-cycle/
- **Improvements to default behavior of opening MHTML files.** MHTML files will continue to open in IE mode if IE mode is enabled, unless the MHTML file was saved from Microsoft Edge (using the Save As or Save Page As options in Microsoft Edge). If the file was saved from Microsoft Edge, it will now open in Microsoft Edge. This change will fix a rendering issue that was observed when opening an MHTML file in IE mode when saved from Microsoft Edge.
- **Restrict private network requests to secure contexts.** Access to resources on local (intranet) networks from pages on the internet requires that those pages be delivered over HTTPS. This change is happening in the Chromium project, on which Microsoft Edge is based. For more information, navigate to the Chrome Platform Status entry. Two compatibility policies are available to support scenarios that need to preserve compatibility with non-secure pages: InsecurePrivateNetworkRequestAllowed and InsecurePrivateNetworkRequestAllowedForUrls.
- **Block mixed content downloads.** Secure pages will only download files hosted on other secure pages, and downloads hosted on non-secure (non-HTTPS) pages will be blocked if initiated from a secure page. This change is happening in the Chromium project, on which Microsoft Edge is based. For more information, navigate to the Google security blog entry.
- **Enable implicit sign-in for on-premises accounts.** By enabling the OnlyOnPremisesImplicitSigninEnabled policy, only on-premises accounts will be enabled for implicit sign-in. Microsoft Edge won't attempt to implicitly sign in to MSA or AAD accounts. Upgrade from on-premises accounts to AAD accounts will be stopped as well.
- **New accessibility settings page.** We have brought accessibility-related settings together on a single page. You can find the new edge://settings/accessibility page under the main settings list. Here you can find settings to make the web page bigger, show a high visibility outline around the area of focus and other settings that can help improve your web browsing experience. We'll continue to add new settings here in future versions of Microsoft Edge.

New Policies

- ApplicationGuardPassiveModeEnabled Ignore Application Guard site list configuration and browse Edge normally
- OnlyOnPremisesImplicitSigninEnabled Only on-premises account enabled for implicit sign-in
- WebRtcRespectOsRoutingTableEnabled Enable support for Windows OS routing table rules when making peer to peer connections via WebRTC

Obsoleted Policy

- UserAgentClientHintsEnabled Enable the User-Agent Client Hints feature

Version 93.0.961.52: September 16

> **IMPORTANT**
>
> This update contains a fix for CVE-2021-30633 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here.

Version 93.0.961.47: September 11

> **IMPORTANT**
>
> This update contains a fix for CVE-2021-30632 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here.

Version 93.0.961.44: September 9

Stable channel security updates are listed here.

Version 93.0.961.38: September 2

Stable channel security updates are listed here.

Feature updates

- **Initial Preferences in Microsoft Edge.** Microsoft Edge now supports a limited number of Initial Preferences (formerly Master Preferences). IT admins can deploy these settings as default before the browser is run for the first time by their users. Additional information here: Configure Microsoft Edge using Initial Preferences settings for the first run.
- **IE mode on Microsoft Edge will support "no-merge" behavior.** For an end-user, when a new browser window is launched from an IE mode application, it will be in a separate session, similar to the no-merge behavior in IE11. You will need to adjust your site list to configure sites that need to prevent session sharing as "no-merge". Behind the scenes, for each window of Microsoft Edge, the first time an IE mode tab is visited within that window, if it is one of the designated "no-merge" sites, that window is locked into a different "no-merge" IE session from all other Microsoft Edge windows at least until the last IE mode tab is closed in that window. This follows previous behavior where users could launch IE with no-merge and could also launch Microsoft Edge without no-merge via other mechanisms. Additional information here: IE mode troubleshooting and FAQ | Microsoft Docs
- **New policy to stop implicit sign in.** The ImplicitSignInEnabled policy allows system administrators to disable implicit sign-in on Microsoft Edge browsers.
- **Policies to bypass ClickOnce and DirectInvoke prompts.** We have updated our policies to enable bypassing ClickOnce's prompts and DirectInvoke's app for specified file types, from specified domains. To do this, you will need to:
  - Enable ClickOnceEnabled or DirectInvokeEnabled

- Enable AutoOpenFileTypes policy and set the list of specific file types that ClickOnce and DirectInvoke should be disabled for
- Enable the AutoOpenAllowedForURLs policy and set the list of specific domains that ClickOnce and DirectInvoke will be disabled for.

Note: AutoOpenAllowedForURLs is a supporter policy for AutoOpenFileTypes. If AutoOpenAllowedForURLs is not set and AutoOpenFileTypes is set, then file types listed will automatically open from all URLs.

- **Tab Groups.** We are turning on tab grouping which provides the ability to categorize tabs into user-defined groups and helps you more effectively find, switch and manage tabs across multiple workstreams.
- **Hide the title bar while using Vertical Tabs.** Get the extra few pixels back by hiding the browser's title bar, while in Vertical Tabs. Now you can go to edge://settings/appearance and under the Customize Toolbar section select the option to hide the title bar while in Vertical Tab mode.
- **Video Picture in Picture (PiP) from hover toolbar.** When you hover over a supported video, a toolbar will appear that allows you to view that video in a PiP window. Please note: this is currently available for Microsoft Edge users on macOS.
- **Removal of 3DES in TLS. Support for the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite will be removed.** This change is happening in the Chromium project, on which Microsoft Edge is based. For more information, navigate to the Chrome Platform Status entry. Additionally, in Microsoft Edge version 93, the TripleDESEnabled policy will be available to support scenarios that need to preserve compatibility with outdated servers. This compatibility policy will become obsolete and stop working in Microsoft Edge version 95. Ensure that you update affected servers before then.

New Policies

- AutoplayAllowlist Allow media autoplay on specific sites
- CECPQ2Enabled CECPQ2 post-quantum key-agreement enabled for TLS
- ConfigureViewInFileExplorer Configure the View in File Explorer feature for SharePoint pages in Microsoft Edge
- DefaultJavaScriptJitSetting Control use of JavaScript JIT
- ShowPDFDefaultRecommendationsEnabled Allow notifications to set Microsoft Edge as default PDF reader
- FeatureFlagOverridesControl Configure users ability to override feature flags
- ImplicitSignInEnabled Enable implicit sign-in
- InternetExplorerIntegrationCloudSiteList Configure the Enterprise Mode Cloud Site List
- InternetExplorerIntegrationSiteListRefreshInterval Configure how frequently the Enterprise Mode Site List is refreshed
- JavaScriptJitAllowedForSites Allow JavaScript to use JIT on these sites
- JavaScriptJitBlockedForSites Block JavaScript from using JIT on these sites
- LocalBrowserDataShareEnabled Enable Windows to search local Microsoft Edge browsing data
- MAUEnabled Always use Microsoft AutoUpdate as the updater for Microsoft Edge
- MSAWebSiteSSOUsingThisProfileAllowed Allow single sign-on for Microsoft sites using this profile
- OneAuthAuthenticationEnforced OneAuth Authentication Flow Enforced for signin
- PasswordGeneratorEnabled Allow users to get a strong password suggestion whenever they are creating an account online
- PrimaryPasswordSetting Configures a setting that asks users to enter their device password while using password autofill
- PrintingWebpageLayout Sets layout for printing
- RemoteDebuggingAllowed Allow remote debugging

- RelaunchWindow Set the time interval for relaunch
- TravelAssistanceEnabled Enable travel assistance
- TripleDESEnabled Enable 3DES cipher suites in TLS
- WAMAuthBelowWin10RS3Enabled WAM for authentication below Windows 10 RS3 enabled

Deprecated Policy

- LegacySameSiteCookieBehaviorEnabled Enable default legacy SameSite cookie behavior setting

Obsoleted Policy

- NewTabPageSetFeedType Configure the Microsoft Edge new tab page experience

Additional Change

- ConfigureShare Add mac platform support
- PasswordMonitorAllowed Add mac platform support

Version 92.0.902.84: August 26

Fixed various bugs & performance issues.

Version 92.0.902.78: August 19

Stable channel security updates are listed here.

Version 92.0.902.73: August 12

Fixed various bugs & performance issues.

Version 92.0.902.67: August 5

Stable channel security updates are listed here.

Version 92.0.902.62: July 29

Fixed various bugs & performance issues.

Modified Policy

- AutoplayAllowed – Setting to "Disabled" now sets media autoplay to "Limit"

Version 92.0.902.55: July 22

Stable channel security updates are listed here.

Feature updates

Users can easily get to Internet Explorer mode on Microsoft Edge. Starting with Microsoft Edge version 92, users can reload a site in Internet Explorer mode on Microsoft Edge instead of relying on the standalone IE 11 application while waiting for a site to be configured in the Enterprise Mode Site List. Users will be prompted to add the site to their local site list such that navigating to the same page in Microsoft Edge will automatically render in IE mode for the next 30 days. You can use the InternetExplorerIntegrationReloadInIEModeAllowed policy to configure this experience and allow access to the IE mode entry points as well as the ability to add sites to the local site list. You can use the InternetExplorerIntegrationLocalSiteListExpirationDays policy to adjust the number of days to keep sites on the local site list. Note that KB5003698 or later is required for Windows 10, version 1909; or KB5003690 or later is required for Windows 10, version 2004, Windows 10, version 20H2, or

Windows 10, version 21H1 for the end-to-end experience. For more information, see Local site list in IE mode.

MHTML files will default to opening in Internet Explorer mode. Starting in Microsoft Edge version 92 Stable, MHTML file types will automatically open in Internet Explorer mode on Microsoft Edge instead of the Internet Explorer (IE11) application. This is most commonly observed while trying to view Outlook emails in a browser. This change will occur only if IE11 is the default handler for this file type. If you'd prefer to change this, you can do so prior to installing the Stable version 92 update using this guidance.

"Disable developer mode extensions" warning can be dismissed for 2 weeks. Beginning with Microsoft Edge version 92, you can snooze the warning "Disable developer mode extensions" for 2 weeks by selecting the option in the warning dialog dropdown.

Manage your extensions right from the toolbar. The all-new extensions menu on the toolbar will allow you to hide/pin extensions easily. The quick links to manage extensions and find new extensions will make it easy for you to find new extensions and manage your existing ones.

Default for autoplay will be set to Limit. To help you maintain your focus online, we have changed the default for autoplaying media to Limit from Allow, beginning with Microsoft Edge version 92.

Payment instruments are now synced across devices. Beginning with Microsoft Edge version 92, you have the option to synchronize your payment information across your signed in devices. Please note: this is a Controlled Feature Rollout. If you don't see this feature, please check back shortly as we continue our rollout. Currently this feature is available only in the US and only for MSA users (not AAD)

Improvements to font rendering. Improvements have been made to the rendering of text to improve clarity and reduce blurriness. Please note: this is a Controlled Feature Rollout. If you don't see this feature, please check back shortly as we continue our rollout.

Toolbar button features like Favorites and Collections will remember the user's choice to pin them to the side of the window. Now enabled by default, if the user chooses to pin a toolbar button, it will always open in the pinned state until they decide to unpin.

Users can now manage the 'Allow single sign-on for work or school sites using this profile' option via group policy. 'Allow single sign-on for work or school sites using this profile' allows non-AAD profiles to be able to use single sign-on for work or school sites using work or school credentials present on the machine. This option shows up for end-users as a toggle in Settings -> Profiles -> Profile Preferences for non-AAD profiles only. You can use the AADWebSiteSSOUsingThisProfileEnabled policy to configure the behavior.

Password health It's important to use strong, unique passwords across different accounts to stay safe online. However, that's easier said than done and most users exhibit poor password habits like using weak passwords that are easy to guess, or reuse the same strong passwords across accounts.

With this latest version of Microsoft Edge, your task of using strong and unique passwords becomes a little bit easier! Microsoft Edge will now tell you whether saved passwords are strong enough and also indicate whether they've been used across multiple sites, helping you stay safer online. You can find your password health information in your list of saved passwords in the edge://settings/passwords page.

Added privacy for your saved passwords If you are using a device you share with others or have left your computer unlocked for whatever reason, you can now opt for a second verification using your device password to avoid others getting access to your website passwords. Simple!

Outlook extension. Stay on top of your Microsoft Outlook inbox, calendar, tasks and more without having to open a new browser window. You can get the new Outlook extension here: Microsoft Outlook - Microsoft Edge Addons

In alignment with the Chromium open source project, Microsoft Edge is updating the way it renders tables on web pages. This change fixes known issues and brings Microsoft Edge closer to the specified way tables are meant to render across the web/other browsers. We recommend that you test

important workflows in your environment for unexpected issues. A full explainer is available here.

New Policies

- AADWebSiteSSOUsingThisProfileEnabled Single sign-on for work or school sites using this profile enabled
- AutomaticHttpsDefault Configure Automatic HTTPS
- HeadlessModeEnabled Control use of the Headless Mode
- InsecurePrivateNetworkRequestsAllowed Specifies whether to allow insecure websites to make requests to more-private network endpoints
- InsecurePrivateNetworkRequestsAllowedForUrls Allow the listed sites to make requests to more-private network endpoints from insecure contexts
- InternetExplorerIntegrationLocalSiteListExpirationDays Specify the number of days that a site remains on the local IE mode site list
- InternetExplorerIntegrationReloadInIEModeAllowed Allow unconfigured sites to be reloaded in Internet Explorer mode
- SharedArrayBufferUnrestrictedAccessAllowed Specifies whether SharedArrayBuffers can be used in a non cross-origin-isolated context

Deprecated Policy

- InternetExplorerIntegrationTestingAllowed Allow Internet Explorer mode testing

Obsoleted Policy

- EnableSha1ForLocalAnchors Allow certificates signed using SHA-1 when issued by local trust anchors

Version 91.0.864.71: July 19

> **IMPORTANT**
> This update contains a fix for CVE-2021-30563 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here.

Version 91.0.864.67: July 8

Fixed various bugs and performance issues.

Version 91.0.864.64: July 2

Fixed various bugs and performance issues.

Version 91.0.864.59: June 24

Stable channel security updates are listed here.

Version 91.0.864.54: June 18

> **IMPORTANT**
> This update contains a fix for CVE-2021-30554 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here.

Version 91.0.864.48: June 11

> **IMPORTANT**
> This update contains a fix for CVE-2021-30551 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here.

Version 91.0.864.41: June 3

Stable channel security updates are listed here.

Version 91.0.864.37: May 27

Stable channel security updates are listed here.

Feature updates

- **Identify network traffic originating from Microsoft Defender Application Guard containers at the proxy level**. Starting with Microsoft Edge version 91, there's built in support to tag network traffic originating from Application Guard containers, allowing enterprises to identify them and apply specific policies.
- **Support option to allow synchronizing Favorites from the host to the Edge Application Guard container**. Starting with Microsoft Edge version 91, users have the option to configure Application Guard to synchronize their favorites from the host to the container. This ensures new favorites appear on the container as well.
- **Starting with Microsoft Edge version 91 the browser will automatically interrupt downloads of types which could harm your computer if those downloads are started without a user interaction and are not supported by SmartScreen Application Reputation check**. Users may override and continue to download by right clicking and choosing "Keep" on the download item. Enterprise administrators may opt out of this behavior by configuring the following policy:
  - ExemptDomainFileTypePairsFromFileTypeDownloadWarnings - Disable download file type extension-based warnings for specified file types on domains

    For more information, see Microsoft Edge Security downloads interruptions.
- **Support for Speech Recognition APIs**. Starting with Microsoft Edge version 91, API support for speech recognition commands on Google.com and similar sites will be added. This feature is limited to a randomly selected group of users who have enabled experimentation. These users are giving feedback to the feature team.
- **Personalize your browser with new theme colors**. Make Microsoft Edge your own with one of the fourteen new theme colors on the Settings -> Appearance page. You can also install custom themes from the Microsoft Edge Add-on site. Learn more

Policy updates

New policies

Six new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added:

- ApplicationGuardTrafficIdentificationEnabled - Application Guard Traffic Identification
- ExplicitlyAllowedNetworkPorts - Explicitly allowed network ports

- ImportStartupPageSettings - Allow importing of startup page settings
- MathSolverEnabled - Let users snip a Math problem and get the solution with a step-by-step explanation in Microsoft Edge
- NewTabPageContentEnabled - Allow Microsoft News content on the new tab page
- NewTabPageQuickLinksEnabled - Allow quick links on the new tab page

Obsoleted Policy

- ProactiveAuthEnabled - Enable Proactive Authentication

Version 90.0.818.66: May 20

Fixed various bugs and performance issues.

Version 90.0.818.62: May 13

Stable channel security updates are listed here.

Version 90.0.818.56: May 6

Fixed various bugs and performance issues.

Version 90.0.818.51: April 29

Stable channel security updates are listed here.

Version 90.0.818.49: April 26

Fixed various bugs and performance issues.

Version 90.0.818.46: April 22

Stable channel security updates are listed here.

Version 90.0.818.42: April 19

Fixed various bugs and performance issues.

Version 90.0.818.41: April 16

> **IMPORTANT**
> This update contains a fix for CVE-2021-21224 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here.

Version 90.0.818.39: April 15

Stable channel security updates are listed here.

Feature updates

- **Single Sign On (SSO) is now available for Azure Active Directory (Azure AD) accounts and Microsoft Account (MSA) on macOS.** A user signed in on Microsoft Edge on macOS will now get

automatically signed into websites that are configured to allow single sign on with Work and Microsoft accounts (for example, bing.com, office.com, msn.com, and outlook.com).

- **Kiosk mode.** Starting with Microsoft Edge version 90, we have locked down the UI print settings to only allow the configured printers and "Print to PDF" options. We have also done improvements within the assigned access single app kiosk mode to restrict the launch of other applications from the browser. For more information about the kiosk mode features please go here.

- **Interrupt Downloads** Starting with Microsoft Edge version 91 the browser will automatically interrupt downloads of types which could harm your computer if those downloads are started without a user interaction and are not supported by SmartScreen Application Reputation check. Users may override and continue to download by right clicking and choosing "Keep" on the download item. Enterprise administrators may opt out of this behavior one of these two policies:

- ExemptDomainFileTypePairsFromFileTypeDownloadWarnings - Disable download file type extension-based warnings for specified file types on domains For more information, see Microsoft Edge Security downloads interruptions

- **Printing**:

  - **New print rasterization mode for non-PostScript printers.** Starting with Microsoft Edge version 90, Admins can use a new policy to define print rasterization mode for their users. This policy controls how Microsoft Edge prints to non-PostScript printers on Windows. Sometimes print jobs on non-PostScript printers need to be rasterized to print correctly. The print options are Full and Fast.

  - **Additional page scaling options for printing.** Users are now able to customize scaling while printing webpages and PDF documents using additional options. The "Fit to Page" option ensures that the webpage or document is fit into the space available in the selected "Paper size" for printing. The "Actual size" option ensures that there are no changes in the size of the contents being printed regardless of the selected "Paper size".

- **Productivity**:

  - **Autofill suggestions are extended to include address fields content from clipboard.** Clipboard content is parsed when you click on a profile/address field (for example, phone, email, zip code, city, state, etc.) to show as autofill suggestions.

  - **Users can search for autofill suggestions even if a form or field isn't detected.** Today if you have your information saved on Microsoft Edge, autofill suggestions pop up automatically and help you save time while filling out forms. In cases where autofill misses a form, or if you want to fetch data in forms that don't typically have autofill (like temporary forms), you can search for your information use autofill.

- **Access downloads from a flyout in the menu bar.** Downloads will appear in the top-right corner with all the active downloads in one place. This menu is easily dismissible so users can continue browsing uninterrupted, and they can monitor overall download progress right from the toolbar. Learn more.

- **Improvements to font rendering.** Starting with Microsoft Edge version 90, we made improvements to the rendering of text to improve clarity and reduce blurriness. Part of the font rendering improvements will land in Beta version 90 but are disabled by default.

- **Kids mode.** We have updated the policy so that when the policy is enabled, it will disable the Kid Mode feature in addition to family safety. More about Kids Mode here

Policy updates

New policies

Eight new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added:

- ApplicationGuardFavoritesSyncEnabled - Application Guard Favorites Sync Enabled
- ApplicationGuardTrafficIdentificationEnabled Application Guard Traffic Identification
- ExplicitlyAllowedNetworkPorts Explicitly allowed network ports
- ImportStartupPageSettings Allow importing of startup page settings
- MathSolverEnabled Let users snip a Math problem and get the solution with a step-by-step explanation in Microsoft Edge
- NewTabPageContentEnabled Allow Microsoft News content on the new tab page
- NewTabPageQuickLinksEnabled Allow quick links on the new tab page
- FetchKeepaliveDurationSecondsOnShutdown- Fetch keepalive duration on shutdown
- ManagedConfigurationPerOrigin - Sets managed configuration values for websites to specific origins
- PrintRasterizationMode - Print Rasterization Mode
- QuickViewOfficeFilesEnabled - Manage QuickView Office files capability in Microsoft Edge
- SSLErrorOverrideAllowedForOrigins - Allow users to proceed from the HTTPS warning page for specific origins
- WindowOcclusionEnabled - Enable Window Occlusion
- WindowsHelloForHTTPAuthEnabled - Windows Hello For HTTP Auth Enabled

Deprecated policies

- ProactiveAuthEnabled Enable Proactive Authentication
- NativeWindowOcclusionEnabled - Enable Native Window Occlusion
- SSLVersionMin- Minimum TLS version enabled

Version 89.0.774.77: April 14

> **IMPORTANT**
> This update contains a fix for CVE-2021-21206 and CVE-2021-21220 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here.

Version 89.0.774.76: April 12

Fixed various bugs and performance issues.

Version 89.0.774.75: April 8

Fixed various bugs and performance issues.

Version 89.0.774.68: April 1

Stable channel security updates are listed here.

Version 89.0.774.63: March 25

Fixed various bugs and performance issues.

Version 89.0.774.57: March 18

Fixed various bugs and performance issues.

Version 89.0.774.54: March 13

> **IMPORTANT**
> This update contains CVE-2021-21193 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here.

Version 89.0.774.50: March 10

Fixed various bugs and performance issues.

Version 89.0.774.48: March 8

Fixed various bugs and performance issues.

Version

> **IMPORTANT**
> This update contains CVE-2021-21166 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Stable channel security updates are listed here.

Resolved issues

- **Taskbar and Start menu shortcut updates and fixes:**
  - Right-clicking the Microsoft Edge shortcut in the Start menu will now properly show the option to unpin Microsoft Edge from the taskbar when it's pinned.
  - Start layouts that include a taskbar configuration to pin Microsoft Edge to the taskbar will no longer result in a second Microsoft Edge shortcut getting pinned to the taskbar.
  - Organizations using Windows Roaming Profiles will no longer see a blank white icon in place of the Microsoft Edge icon on the taskbar when their users log on to Windows.

Feature updates

- **Kiosk mode enables additional lockdown capabilities**. Starting with Microsoft Edge version 89, we have added additional lockdown capabilities within kiosk mode to enable customers to get the job done in a productive and more secure experience. Learn more.
- **The Enterprise Mode Site List Manager tool will be available in the browser through the *edge://compat* page**. You can use this tool to create, edit and export your site list XML for Internet Explorer mode on Microsoft Edge. You can enable access to this tool as needed through group policy. Learn More.
- **Improve browser performance with sleeping tabs**. Sleeping tabs improves browser performance by putting inactive tabs to sleep to free up system resources like memory and CPU so active tabs or other

applications can use them. Users can prevent sites from going to sleep and configure the length of time before an inactive tab goes to sleep. To keep users in their flow, there are also heuristics to prevent certain sites from going to sleep, such as intranet sites. This feature can be managed with group policies.

- **Reset your Microsoft Edge sync data in the cloud manually**. We are introducing a way to reset your Microsoft Edge sync data from within the product. This ensures that your data is cleared from Microsoft services, as well as resolving certain product issues that previously required a support ticket.
- **Intelligent enablement of Single sign-on (SSO) for all Windows Azure Active Directory (Azure AD) accounts for users with a single non-Azure AD Microsoft Edge profile**. Automatically turn this setting on for users that might benefit the most from this feature. If a user has only one Microsoft Edge profile (and it's not Azure AD or Kids Mode), the setting will be automatically turned on when Microsoft Edge launches. This auto-toggle will also automatically turn off if a user later chooses to sign into a different Microsoft Edge profile with an Azure AD account. Users can manually update their preferences for this feature in **Settings > Profiles >Profile Preferences > Allow single sign-on for work or school sites using this profile**.
- **Improvements to text selection experience within PDF documents**. Users will begin to get a smoother and more consistent text selection experience across PDF documents opened in Microsoft Edge starting with version 89.
- **Date of birth field now supported in autofill**. Today Microsoft Edge helps you save time and effort while filling out forms and creating accounts online by auto filling your data like addresses, names, phone numbers, etc. Starting with Microsoft Edge version 89, we are adding support for another field that you can have saved and auto-filled - date of birth. You can view, edit and delete this information anytime in your profile settings.

Policy updates

New policies

Seven new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added.

- BrowsingDataLifetime - Browsing Data Lifetime Settings
- MAMEnabled - Mobile App Management Enabled
- DefinePreferredLanguages - Define an ordered list of preferred languages that websites should display in if the site supports the language
- ShowRecommendationsEnabled - Allow recommendations and promotional notifications from Edge
- PrintingAllowedBackgroundGraphicsModes - Restrict background graphics printing mode
- PrintingBackgroundGraphicsDefault - Default background graphics printing mode
- SmartActionsBlockList - Block smart actions for a list of services

Obsoleted policies

The following policies are obsoleted.

- ForceLegacyDefaultReferrerPolicy - Use a default referrer policy of no-referrer-when-downgrade
- MetricsReportingEnabled - Enable usage and crash-related data reporting
- SendSiteInfoToImproveServices - Send site information to improve Microsoft services

Version 88.0.705.81: February 25

Fixed various bugs and performance issues.

Version 88.0.705.74: February 17

Stable channel security updates are listed here.

Version 88.0.705.68: February 11

Fixed various bugs and performance issues.

Version 88.0.705.63: February 5

> **IMPORTANT**
> This update contains CVE-2021-21148 which has been reported by the Chromium team as having an exploit in the wild.

Stable channel security updates are listed here.

Version 88.0.705.62: February 4

Stable channel security updates are listed here.

Fixed various bugs and performance issues.

Version 88.0.705.56: January 28

Fixed various bugs and performance issues.

Version 88.0.705.53: January 26

Fixed various bugs and performance issues.

Version 88.0.705.50: January 21

Stable channel security updates are listed here.

Feature updates

- **Deprecations:**
  - Deprecate support for FTP protocol. Support for the legacy FTP protocol has been removed from Microsoft Edge. Attempting to navigate to an FTP link will result in the browser directing the Operating System to open an external application to handle the FTP link. Alternatively, IT administrators can configure Microsoft Edge to use IE Mode for sites that rely on the FTP protocol.
  - Adobe Flash support will be removed. Starting with Microsoft Edge Beta version 88, Adobe Flash capability and support will be removed. Learn more: Update on Adobe Flash Player End of Support - Microsoft Edge Blog (windows.com)
- **Authentication:**
  - Single Sign On (SSO) now available for Azure Active Directory (Azure AD) accounts and Microsoft Account (MSA) on down-level Windows. A user signed in on Microsoft Edge on down-level Microsoft Windows (7, 8.1) will now get automatically signed into websites that are configured to allow single sign on with Work and Microsoft accounts (e.g., bing.com, office.com, msn.com, outlook.com).
    Note: A user may have to sign out and then sign back in if they'd signed into Microsoft Edge in a version prior to Microsoft Edge 88 to leverage this feature.
  - Single sign-on (SSO) to work sites using any Windows Azure Active Directory (Azure AD) accounts on system in non-Azure AD Microsoft Edge profiles. This feature can be enabled for any profile that isn't signed-in with a work/school account and is not guest or in-private and allows the use of any signed-in work/school account on operating system with that profile. This feature can be

configured in **Settings** > **Profiles** > **Profile Preferences** > **Allow single sign-on for work or school sites using this profile**.

> **NOTE**
> "Single sign-on (SSO) for all Windows accounts using the Microsoft Edge profile" is an update to the January 21 release notes.

- **Kiosk mode option to end session**. The "End session" button is now available in a kiosk mode public browsing experience. This feature ensures that browser data and settings are deleted when Microsoft Edge is closed. Learn more about kiosk mode features and roadmap, Configure Microsoft Edge kiosk mode.
- **Security and Privacy:**
  - Alerts are generated if a user's password is found in an online leak. User passwords are checked against a repository of known-breached credentials and sends the user an alert if a match is found. To ensure security and privacy, user passwords are hashed and encrypted when they're checked against the database of leaked credentials.
  - Automatically upgrade mixed content. Secure pages delivered over HTTPS may contain references images that are served over non-secure HTTP. To improve privacy and security in Microsoft Edge 88, those images will be retrieved over HTTPS instead. If the image is not available over HTTPS, it will not be loaded.
  - View site permissions by site and by recent activity. Starting with Microsoft Edge 88, users will be able to manage site permissions more easily. They will be able to view permissions by web site rather than just permission type. Additionally, we've added a recent activity section that will show a user all the recent changes to their site permissions.
  - Increased controls for browser cookies. Starting with Microsoft Edge 88, users can delete third party cookies without affecting first party cookies. Users will also be able to filter their cookies by first or third party and sort by name, number of cookies, and the amount of data stored and last modified.
- **Passwords:**
  - Password Generator. Microsoft Edge offers a built-in strong password generator that you can use when signing up for a new account or when changing an existing password. Just look for the browser-suggested password drop down in the password field and when selected, it will automatically save to the browser and sync across devices for easy future use.
  - Password Monitor. When any of your passwords saved to the browser matches with those seen in the list of leaked credentials, Microsoft Edge will notify you and prompt you to update your password. Password Monitor scans for matches on your behalf and is on by default.
  - Edit Password. You can now edit your saved passwords directly in Microsoft Edge Settings. Any time a password has been updated outside of Microsoft Edge, it's easy to replace the saved older password with the new one by editing the saved entry in Settings.
- **Improve Microsoft Edge startup speed with startup boost**. To improve Microsoft Edge startup speed, we've developed a feature named startup boost. Startup boost makes Microsoft Edge launch faster by enabling Microsoft Edge to run in the background. Note: This feature is limited to a randomly selected group of users who have enabled experimentation. These users are giving feedback to the feature team.
- **Productivity:**
  - Improve productivity and multi-tasking with vertical tabs. As the number of horizontal tabs grows, site titles start to get cut off and tab controls are lost as each tab shrinks. This interrupts user workflow as they spend more time finding, switching, and managing their tabs and less time on the task at hand.

Vertical tabs let users move their tabs to the side, where vertically aligned icons and longer site titles make it easier to quickly scan, identify and switch to the tab they want to open.

  - Auto filling the date of birth field. Microsoft Edge already helps save time and effort while filling out forms and creating accounts online by auto filling user data such as addresses, names, phone numbers, etc. Microsoft Edge now supports the date of birth field which users can save and auto fill. A user can view, edit and delete this information anytime in their profile settings.
  - Improvements to Recently closed in History. Recently closed now keeps the last 25 tabs and windows from any past browsing session rather than just the previous session. Users can select Recently closed in the new History experience to see all the tabs that were open.
  - "Your day at a glance" feature enabled by default. Starting with Microsoft Edge version 88, information workers can benefit from intelligent productivity features on their New tab page (NTP). Microsoft Edge 87 users will also experience these features within 2 weeks after Microsoft Edge 88 release. We offer users signed in with their work or school account personalized and relevant content powered by their M365 Graph. Users can quickly scan their "Your day at a glance" modules to easily track their meetings and recent work as well as quickly launch the applications they want to use.
- **History and open tabs sync**. History and open tabs sync is now available for users to enjoy. Enabling these features will help users pick up where they left off by making their browsing history and open tabs available on all their syncing devices. We've updated sync and browser history policies, so now users are connected and productive across any devices by using Microsoft Edge. Learn more.
- **PDF:**
  - PDF document display in book view (two page). Starting with Microsoft Edge version 88, users can view PDF documents in a single page or in the two page book view. To change the view, click the **Page View** button in the toolbar.
  - Anchored text notes support for PDF files. Starting with Microsoft Edge version 87, users can add typed text notes on any piece of text in PDF files.
- **Fonts:**
  - Browser icons are updated to the Fluent design system. As part of our continued work around Fluent Design in the browser, we've made changes to closer align icons to the new Microsoft icon system. These changes will impact many of our high-touch user interfaces, including tabs, address bar, as well as navigational and wayfinding icons found in our various menus.
  - Improved font rendering. Text rendering is improved for better clarity and to reduce blurriness.

Policy updates

New policies

Eighteen new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added.

- BasicAuthOverHttpEnabled - Allow Basic authentication for HTTP.
- BlockExternalExtensions - Blocks external extensions from being installed.
- InternetExplorerIntegrationLocalFileAllowed - Allow launching of local files in Internet Explorer mode.
- InternetExplorerIntegrationLocalFileExtensionAllowList - Open local files in Internet Explorer mode file extension allow list.
- InternetExplorerIntegrationLocalFileShowContextMenu - Show context menu to open a link in Internet Explorer mode.
- IntranetRedirectBehavior - Intranet Redirection Behavior.
- PrinterTypeDenyList - Disable printer types on the deny list.
- ShowMicrosoftRewards - Show Microsoft Rewards experiences.
- SleepingTabsEnabled - Configure Sleeping Tabs.
- SleepingTabsTimeout - Set the background tab inactivity timeout for Sleeping Tabs.

- SleepingTabsBlockedForUrls - Block Sleeping Tabs on specific sites.
- StartupBoostEnabled - Enable startup boost.
- TargetBlankImpliesNoOpener - Do not set window.opener for links targeting _blank.
- UpdatePolicyOverride - Specifies how Microsoft Edge Update handles available updates from Microsoft Edge.
- VerticalTabsAllowed - Configures availability of a vertical layout for tabs on the side of the browser.
- WebRtcAllowLegacyTLSProtocols - Allow legacy TLS/DTLS downgrade in WebRTC.
- WebWidgetAllowed - Enable the Web widget.
- WebWidgetIsEnabledOnStartup - Allow the Web widget at Windows startup.

Deprecated Policies

- ProactiveAuthEnabled - Enable Proactive Authentication.
- ProxyBypassList - Configure proxy bypass rules.
- ProxyMode - Configure proxy server settings.
- ProxyPacUrl - Set the proxy .pac file URL.
- ProxyServer - Configure address or URL of proxy server.
- WebDriverOverridesIncompatiblePolicies - Allow WebDriver to Override Incompatible Policies.

Obsoleted Policies

- AllowPopupsDuringPageUnload - Allows a page to show popups during its unloading.
- DefaultPluginsSetting - Default Adobe Flash setting.
- PluginsAllowedForUrls - Allow the Adobe Flash plug-in on specific sites.
- PluginsBlockedForUrls - Block the Adobe Flash plug-in on specific sites.
- RunAllFlashInAllowMode - Extend Adobe Flash content setting to all content.

Version 87.0.664.75: January 7

Stable channel security updates are listed here.

Version 87.0.664.66: December 17

Fixed various bugs and performance issues.

Version 87.0.664.60: December 10

Fixed various bugs and performance issues.

Version 87.0.664.57: December 7

Fixed various bugs and performance issues. Stable channel security updates are listed here.

Version 87.0.664.55: December 3

Fixed various bugs and performance issues. The following feature was updated for this release.

- **Shopping is enabled by default**. Starting with Microsoft Edge version 87, enterprise users can benefit from shopping in Microsoft Edge. With Shopping features, Microsoft Edge helps users find coupons and better prices while shopping online. (The coupon experience was released with Stable version 87.0.664.41). The price comparison experience is now available with this update. This feature can be configured using the EdgeShoppingAssistantEnabled policy. See our Blog and Learn More about Microsoft Shopping.

Version 87.0.664.52: November 30

Fixed various bugs and performance issues.

Version 87.0.664.47: November 23

Fixed various bugs and performance issues.

Version 87.0.664.41: November 19

Stable channel security updates are listed here.

Feature updates

- **Automatic redirection for incompatible sites from Internet Explorer to Microsoft Edge**. Starting with the Microsoft Edge 87 Stable update, public websites that show an incompatibility message on Internet Explorer will be automatically redirected to Microsoft Edge. To learn more and to configure this experience, see Redirecting incompatible sites.
- **Kiosk mode privacy features enabled**. Starting with Microsoft Edge version 87, kiosk mode features that will help enterprises around the privacy of user data will be enabled. These features will enable experiences such as clear the user data on exit, delete downloaded files and to reset the configured start experience after a specified amount of idle time. Learn more about how to Configure Microsoft Edge kiosk mode
- **Shopping features enabled by default**. Starting with Microsoft Edge version 87 enterprise users can also benefit from shopping in Edge. With Shopping features, Microsoft Edge helps users to find coupons and better prices while shopping online. Coupon experience is available with this update and price comparison will be released in upcoming updates for Microsoft Edge 87. This feature can be configured through EdgeShoppingAssistantEnabled policy. See our Blog and Learn More about Microsoft Shopping.
- **ClickOnce deployment enabled by default**. ClickOnce is enabled by default in Microsoft Edge 87, which reduces the barriers for enterprises to deploy software and better align with Microsoft Edge Legacy browser behavior. Starting in Microsoft Edge 87, the ClickOnceEnabled policy's "Not configured" state will reflect the new default ClickOnce state of Enabled (as compared to the previous default state of Disabled).
- **The enterprise new tab page (NTP) integrates productivity with customizable, work-relevant feed content**. The enterprise NTP blends the Office 365 productivity page we offer to users signed in with their work or school account with personalized, work-relevant company and industry feeds that are organized in a single page. Users will be able to recognize the familiar Office 365 content and Microsoft Search for Business powered by Bing. In addition, they can easily customize "My Feed" by choosing the most relevant content to them from the available content and modules for their organization. IT Administrators can control the News feed settings for their organization, including the selected industry for the Edge new tab page by going to Microsoft 365 admin center. Learn more
- **Privacy and Security:**
  - Support TLS Token Binding for policy-configured sites. TLS Token binding helps prevent token theft attacks to ensure that cookies can't be reused from a device other than the device upon which they were initially set. The use of TLS token binding requires setting the AllowTokenBindingForUrls policy and requires that the sites listed support this feature.
- **Keyboard support for highlighter on PDF files**. Users can use their keyboard keys to highlight any text on a PDF.
- **Printing:**
  - Choose which side to flip on when printing on both sides. Users can choose to flip on the long side or the short side of a sheet when printing on both sides.
  - Choose print rasterization mode for the enterprise. Control how Microsoft Edge prints to a non-

PostScript printer on Windows. Sometimes print jobs on non-PostScript printers need to be rasterized to print correctly. The print options are "Full" and "Fast".

Policy updates

New policies

Ten new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added.

- ConfigureFriendlyURLFormat - Configure the default paste format of URLs copied from Microsoft Edge, and determine if additional formats will be available to users.
- EdgeShoppingAssistantEnabled - Shopping in Microsoft Edge enabled.
- HideInternetExplorerRedirectUXForIncompatibleSitesEnabled - Hide the one-time redirection dialog and the banner on Microsoft Edge.
- KioskAddressBarEditingEnabled - Configure address bar editing for kiosk mode public browsing experience.
- KioskDeleteDownloadsOnExit - Delete files downloaded as part of kiosk session when Microsoft Edge closes.
- PasswordRevealEnabled - Enable Password reveal button.
- RedirectSitesFromInternetExplorerPreventBHOInstall - Prevent install of the browser helper object (BHO) to redirect incompatible sites from Internet Explorer to Microsoft Edge.
- RedirectSitesFromInternetExplorerRedirectMode - Redirect incompatible sites from Internet Explorer to Microsoft Edge.
- SpeechRecognitionEnabled - Configure Speech Recognition.
- WebCaptureEnabled - Enable web capture feature in Microsoft Edge.

Deprecated Policy

NewTabPageSetFeedType - Configure the Microsoft Edge new tab page experience.

Obsoleted Policy

EnableDeprecatedWebPlatformFeatures - Re-enable deprecated web platform features for a limited time.

Version 86.0.622.69: November 13

> **IMPORTANT**
> This update contains CVE-2020-16013 and CVE-2020-16017, that have been reported by the Chromium team as having an exploit in the wild.

Stable channel security updates are listed here.

Version 86.0.622.68: November 11

Stable channel security updates are listed here

Version 86.0.622.63: November 4

> **IMPORTANT**
> This update contains CVE-2020-16009, that has been reported by the Chromium team as having an exploit in the wild.

Stable channel security updates are listed here.

Version 86.0.622.61: November 2

Fixed various bugs and performance issues.

Version 86.0.622.58: October 29

Fixed various bugs and performance issues.

Version 86.0.622.56: October 27

Fixed various bugs and performance issues.

Version 86.0.622.51: October 22

Stable channel security updates are listed here

Version 86.0.622.48: October 20

Fixed various bugs and performance issues.

Version 86.0.622.43: October 15

Fixed various bugs and performance issues.

Version 86.0.622.38: October 9

Security updates are listed here

Feature updates

- **Roll back to previous Microsoft Edge version.** The rollback feature lets administrators revert to a known good version of Microsoft Edge if there's an issue in the latest version of Microsoft Edge. **Note:** Stable version 86.0.622.38 is the first version you can roll back to, which means that Stable version 87 is the first version ready to rollback from. Learn more.
- **Enforce enabling Sync by default across the enterprise.** Administrators can enable synchronization for Azure Active Directory (Azure AD) accounts by default with the ForceSync policy.
- **Automatic profile switching on Windows 7 and 8.1.** The automatic profile switching currently available in Microsoft Edge on Windows 10 is extended to downlevel Windows (Windows 7 and 8.1). For more information, see the automatic profile switching blog post.
- **SameSite=Lax Cookies By Default**. To improve web security and privacy, cookies will now default to SameSite=Lax handling by default. This means that cookies will only be sent in a first-party context and will be omitted for requests sent to third-parties. This change can cause compatibility impact on websites that require cookies for third-party resources to function correctly. To permit such cookies, web developers can mark cookies which should be set from and sent to third-party contexts by adding explicit `SameSite=none` and `Secure` attributes when the cookie is set. Enterprises that wish to exempt certain sites from this change can do so using the LegacySameSiteCookieBehaviorEnabledForDomainList policy, or can opt-out of the change across all sites using the LegacySameSiteCookieBehaviorEnabled policy.
- **Remove the HTML5 Application Cache API.** Beginning with Microsoft Edge version 86, the legacy Application Cache API that enables offline use of web pages is being removed from Microsoft Edge. Web Developers should review the WebDev documentation for information on replacing the Application Cache API with Service Workers. Important: You can request an AppCache OriginTrial Token that allows sites to continue to use the deprecated Application Cache API until Microsoft Edge version 90.
- **Privacy and Security:**

    - Replace MetricsReportingEnabled and SendSiteInformationToImproveServices policies for downlevel Windows and macOS. These policies are deprecated in Microsoft Edge version 86 and will become obsolete in Microsoft Edge version 89.
      These policies are replaced by Allow Telemetry on Windows 10, and the new DiagnosticData policy for all other platforms. This will let users manage the diagnostic data that gets sent to Microsoft for Windows 7, 8, 8.1 and macOS.
    - Secure DNS (DNS-over-HTTPS) support. Beginning with Microsoft Edge version 86, settings to control Secure DNS on un-managed devices is available. These settings aren't accessible to users on managed devices, but IT admins can enable or disable Secure DNS using the dnsoverhttpsmode group policy.
- **Internet Explorer mode:** Let users use the Microsoft Edge User Interface (UI) to test sites in Internet Explorer mode. Beginning with Microsoft Edge version 86, administrators can enable a UI option for their users to load a tab in Internet Explorer mode for testing purposes or as a stopgap until sites are added to the site list XML.
- **PDF updates:**
    - Table of contents for PDF Documents. Beginning with version 86, Microsoft Edge has added support for table of contents that lets users easily navigate through PDF documents.
    - Access all PDF functionalities on small form factor screens. Access all the capabilities of the Microsoft Edge PDF reader on devices with small screen sizes.
    - Pen support for highlighter on PDF files. With this update, users can use their digital pen to directly highlight text on PDF files, in the same way they would with a physical highlighter and paper.
    - Improved PDF scrolling. You will now be able to experience stutter free scrolling while navigating through long PDF documents.
- **Users will see auto complete suggestions when they start typing a search query on the Microsoft Edge Add-ons website.** Auto complete will help users quickly complete their search query without having to type the entire string. This will be helpful because users won't have to remember correct spellings and they can choose from the available options that are displayed.
- **Add a custom image to the New Tab Page (NTP) using a group policy.** Beginning with Microsoft Edge version 86 the NTP has an option to replace the default image with a custom user-supplied image. The ability to manage the properties of this image is also supported by the group policy.
- **Match customized keyboard shortcuts to VS Code.** Microsoft Edge DevTools now supports customizing keyboard shortcuts in the DevTools to match with your editor/IDE. (In Microsoft Edge 84, we added the ability to match DevTools keyboard shortcuts to VS Code).
- **Delete downloads from disk using download manager.** Users are now able to delete their downloaded files from their disk without leaving the browser. The new Delete downloads functionality exists within the context menu of downloads shelf or the downloads page.

Policy updates

New policies

Twenty-three new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added.

- CollectionsServicesAndExportsBlockList - Block access to a specified list of services and export targets in Collections.
- DefaultFileSystemReadGuardSetting - Control use of the File System API for reading.
- DefaultFileSystemWriteGuardSetting - Control use of the File System API for writing.
- DefaultSensorsSetting - Default sensors setting.
- DefaultSerialGuardSetting - Control use of the Serial API.
- DiagnosticData - Send required and optional diagnostic data about browser usage.

- EnterpriseModeSiteListManagerAllowed - Allow access to the Enterprise Mode Site List Manager tool.
- FileSystemReadAskForUrls - Allow read access via the File System API on these sites.
- FileSystemReadBlockedForUrls - Block read access via the File System API on these sites.
- FileSystemWriteAskForUrls - Allow write access to files and directories on these sites.
- FileSystemWriteBlockedForUrls - Block write access to files and directories on these sites.
- ForceSync - Force synchronization of browser data and do not show the sync consent prompt.
- InsecureFormsWarningsEnabled - Enable warnings for insecure forms.
- InternetExplorerIntegrationTestingAllowed - Allow Internet Explorer mode testing.
- SpotlightExperiencesAndRecommendationsEnabled - Choose whether users can receive customized background images and text, suggestions, notifications, and tips for Microsoft services.
- NewTabPageAllowedBackgroundTypes - Configure the background types allowed for the new tab page layout.
- SaveCookiesOnExit - Save cookies when Microsoft Edge closes.
- SensorsAllowedForUrls - Allow access to sensors on specific sites.
- SensorsBlockedForUrls - Block access to sensors on specific sites.
- SerialAskForUrls - Allow the Serial API on specific sites.
- SerialBlockedForUrls - Block the Serial API on specific sites.
- UserAgentClientHintsEnabled - Enable the User-Agent Client Hints feature.
- UserDataSnapshotRetentionLimit - Limits the number of user data snapshots retained for use in case of emergency rollback.

Deprecated Policies

- MetricsReportingEnabled - Enable usage and crash-related data reporting.
- SendSiteInfoToImproveServices - Send site information to improve Microsoft services.

Obsoleted Policy

TLS13HardeningForLocalAnchorsEnabled - Enable a TLS 1.3 security feature for local trust anchors.

Version 85.0.564.70: October 6

Fixed various bugs and performance issues.

Version 85.0.564.68: October 1

Fixed various bugs and performance issues.

Version 85.0.564.63: September 23

Security updates are listed here

Version 85.0.564.51: September 9

Security updates are listed here

Version 85.0.564.44: August 31

Fixed various bugs and performance issues.

Version 85.0.564.41: August 27

Security updates are listed here

Feature updates

- **On-premises synchronization of Favorites and Settings**. Now you can synchronize browser favorites and settings between Active Directory profiles within your own environment without the need for cloud sync.
- **Microsoft Edge group policy support for trusting site + app combos to launch without a confirmation prompt.**. Group policy support added that lets administrators add site + app combos that are trusted to launch without the confirmation prompt. This adds the ability for administrators to configure trusted protocol/origin combinations (such as Microsoft 365 apps) for their end-users to suppress the confirmation prompt when navigating to a URL that contains an app protocol.
- **PDF Highlighter tool**. This tool can be added to the toolbar for PDFs to easily highlight important text.
- **The Storage Access API is available**. The Storage Access API allows access to first-party storage in a third-party context when a user has provided a direct intent to allow storage that would otherwise be blocked by the browser's current configuration. For more information, see Storage Access API.
- **Send to OneNote is available for Microsoft Edge Collections**. Everyone's excited to be able to send the information they've gathered in Collections to OneNote, where they can append it to a larger project and collaborate with others! And even more importantly, in Microsoft Edge 85, you'll be able send content to *Office for Mac* products (Word, Excel, and OneNote) for both Microsoft account and Azure Active Directory.
- **DevTools updates**. For details about the following updates, see What's New In DevTools (Microsoft Edge 85).
    - Microsoft Edge DevTools supports Surface Duo emulation. The Microsoft Edge DevTools can emulate the Surface Duo so you can test how your web content will look on dual-screen devices. To turn on this experiment in DevTools, enter Device Mode by pressing Ctrl+Shift+M on Windows or Command+Shift+M on macOS, and then select Surface Duo from the device drop-down list.
    - Microsoft Edge DevTools lets you match keyboard shortcuts to VS Code. The Microsoft Edge DevTools supports customizing keyboard shortcuts in the DevTools to match your editor/IDE. In Microsoft Edge 85, we are adding the ability to match DevTools keyboard shortcuts to VS Code. This change will help increase productively across VS Code and DevTools.

Policy updates

New policies

Thirteen new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added.

- AutoLaunchProtocolsFromOrigins - Define a list of protocols that can launch an external application from listed origins without prompting the user.
- AutoOpenAllowedForURLs - URLs where AutoOpenFileTypes can apply.
- AutoOpenFileTypes - List of file types that should be automatically opened on download.
- DefaultSearchProviderContextMenuAccessAllowed - Allow default search provider context menu search access.
- EnableSha1ForLocalAnchors - Allow certificates signed using SHA-1 when issued by local trust anchors.
- IntensiveWakeUpThrottlingEnabled - Control the IntensiveWakeUpThrottling feature.
- NewTabPagePrerenderEnabled - Enable preload of the new tab page for faster rendering.
- NewTabPageSearchBox - Configure the new tab page search box experience.
- PasswordMonitorAllowed - Allow users to be alerted if their passwords are found to be unsafe.
- RoamingProfileSupportEnabled - Enable using roaming copies for Microsoft Edge profile data.
- RoamingProfileLocation - Set the roaming profile directory.
- TLSCsipherSuiteDenyList - Specify the TLS cipher suites to disable.

Obsoleted policies

- EnableDomainActionsDownload - Enable Domain Actions Download from Microsoft.
- WebComponentsV0Enabled - Re-enable Web Components v0 API until M84.
- WebDriverOverridesIncompatiblePolicies- Allow WebDriver to Override Incompatible Policies.

Version 84.0.522.63: August 20

Security updates are listed here.

Version 84.0.522.61: August 17

Fixed various bugs and performance issues.

Version 84.0.522.59: August 11

Security updates are listed here

Version 84.0.522.58: August 10

Fixed various bugs and performance issues.

Version 84.0.522.52: August 1

Fixed various bugs and performance issues.

Version 84.0.522.50: July 31

Fixed various bugs and performance issues.

Version 84.0.522.49: July 29

Security updates are listed here

Version 84.0.522.48: July 28

Fixed various bugs and performance issues.

Version 84.0.522.44: July 23

Fixed various bugs and performance issues.

Version 84.0.522.40: July 16

Security updates are listed here

Feature updates

- This version of Microsoft Edge provides improved site list download times for Internet Explorer mode. We've reduced download delay for the Internet Explorer mode site list to 0 seconds (down from a 60-second wait) in the absence of a cached site list. We've also added group policy support for cases when Internet Explorer mode home page navigations need to be delayed until the site list is downloaded. For more information, see the DelayNavigationsForInitialSiteListDownload policy.
- Microsoft Edge now allows users to sign-into the browser when it's "run as administrator" on Windows 10. This will help customers running Microsoft Edge on Windows server or in remote-desktop and

sandbox scenarios.

- Microsoft Edge now provides full mouse support when in full screen mode. Now you can use your mouse to access tabs, the address bar, and other items without having to exit full screen mode.
- Online purchase improvement. Add custom nicknames to saved debit or credit cards. Now you can distinguish and differentiate your credit cards when making online purchases. Nicknaming your debit or credit cards lets you choose the correct card when using autofill to select a payment method.
- TLS/1.0 and TLS/1.1 are disabled by default. The SSLVersionMin policy permits re-enabling of TLS/1.0 and TLS/1.1. This policy will remain available until at least Microsoft Edge version 88. For more information, see Site compatibility-impacting changes coming to Microsoft Edge.
- Collections improvements:
  - A note capability is added that lets you add a note or comment to an item in a collection. Notes are grouped together and stay attached to an item even if you sort the items in a collection. To try this new feature, right-click on an item and select "Add note".
  - You can change the background color of notes in collections. You can use color coding to help you organize information and increase productivity.
  - There are noticeable performance improvements, which lets you export your collections to Excel in less time than in previous versions of Microsoft Edge.
- Additional Microsoft Edge API support:
  - The Storage Access API is enabled for experimentation. This feature is enabled for home users and Enterprise users with the ExperimentationAndConfigurationServiceControl policy set to "Full". This feature will be enabled by default for all users in Microsoft Edge Stable Channel version 85.

    As privacy is becoming increasingly important to users, requests for stricter browser defaults and user opt-in settings like blocking all third-party storage access are increasingly common. While these settings help improve privacy and block unwanted access by unknown or untrusted parties, they can have unwanted side effects such as blocking access to content the user may want to view (for example, social media and embedded media content.)

    The Storage Access API allows access to first-party storage in a third-party context when a user provides a direct intent to allow storage that would otherwise be blocked by the browser's current configuration. For more information, see Storage Access API.
  - The Native File System API, which means you can give sites permissions to edit files or folders via the Native File System API.
- PDF improvements:
  - Read Aloud for PDF lets users listen to PDF content while carrying out other tasks that may be important for them. It also helps audio visual learners focus on reading the content, making learning easier.
  - PDF file editing is improved. Now you can save an edit made to a PDF back to the file instead of saving a copy each time you edit the PDF.
- Microsoft Edge now enables Translation in the Immersive Reader. When a user opens the Immersive Reader view, they get the option to translate the page to their desired language.
- Several DevTools updates, including support for customizing keyboard shortcuts to match VS Code and viewing the DevTools in high contrast. For more details, see What's New In DevTools (Microsoft Edge 84).

Policy updates

New policies

Seven new policies were added. Download the updated Administrative Templates from the Microsoft Edge

Enterprise landing page. The following new policies were added.

- AppCacheForceEnabled - Allows the AppCache feature to be re-enabled, even if it's turned off by default.
- ApplicationGuardContainerProxy - Configure the settings for the Application Guard Container Proxy.
- DelayNavigationsForInitialSiteListDownload - Require that the Enterprise Mode Site List is available before tab navigation.
- WinHttpProxyResolverEnabled - Use the Windows proxy resolver.
- InternetExplorerIntegrationEnhancedHangDetection - Configure enhanced hang detection for Internet Explorer mode.
- NativeWindowOcclusionEnabled - To reduce CPU and power consumption Microsoft Edge will detect when a window is covered by other windows, and will suspend work painting pixels.
- NavigationDelayForInitialSiteListDownloadTimeout - Set a timeout for delay of tab navigation for the Enterprise Mode Site List.

Deprecated policies

- AllowSyncXHRInPageDismissal - Allow pages to send synchronous XHR requests during page dismissal.
- BuiltinCertificateVerifierEnabled - Determines whether the built-in certificate verifier will be used to verify server certificates.
- StricterMixedContentTreatmentEnabled - Enable stricter treatment for mixed content.

Obsoleted policy

ForceNetworkInProcess - Force networking code to run in the browser process.

Version 83.0.478.64: July 13

Fixed various bugs and performance issues.

Version 83.0.478.61: July 7

Fixed various bugs and performance issues.

Version 83.0.478.58: June 30

Fixed various bugs and performance issues.

Version 83.0.478.56: June 24

Fixed various bugs and performance issues.

Security updates are listed here

Version 83.0.478.54: June 17

Security updates are listed here

Version 83.0.478.50: June 15

Fixed various bugs and performance issues.

Version 83.0.478.45: June 4

Security updates are listed here

Version 83.0.478.44: June 1

Fixed various bugs and performance issues.

Version 83.0.478.37: May 21

Security updates are listed here

Feature updates

- Microsoft Edge updates will now roll out gradually. Going forward, updates for Microsoft Edge will be rolled out to our users over a period of a few days. This enables us to protect more of you from accidental buggy updates, which improves your update experience. As a user you will continue to get seamless auto-updates. If your organization isn't enrolled for auto-updates you won't be affected by this change. To learn more, see the progressive rollouts article.
- Microsoft Defender SmartScreen improvements: Made several improvements to the Microsoft Defender SmartScreen service, such as improved protection from malicious sites that redirect when loading, and top-level frame blocking, which completely replaces malicious sites with the Microsoft Defender SmartScreen safety page. The top-level frame blocking prevents audio and other media from the malicious site from playing which gives an easier and less confusing experience.
- In response to user feedback, users can now exempt certain cookies from automatically clearing when the browser closes. This option is helpful if there's a site that users don't want to be signed out of, but still want to have all the other cookies cleared when the browser closes. To use this feature, go to *edge://settings/clearBrowsingDataOnClose* and enable the "Cookies and other site data" toggle.
- Automatic Profile Switching is now available to help you get to your work content more easily across profiles. If you use multiple profiles at work, you can check it out by navigating to a site requiring authentication from your work or school account while on your personal profile. When we detect this, you will receive a prompt to switch to your work profile to access that site without having to authenticate to it. When you choose the work profile you want to switch to, the website will simply open in your work profile. This profile switching capability will help you keep your work and personal data separate and help you get to your work content more effortlessly. If you don't want the feature to prompt you to switch profiles, you can choose the don't ask me again option and it will get out of your way.
- Collections feature improvements:
    - You can use drag and drop to add an item to a collection without opening the collection. During the drag and drop you can also choose a location in the collection list where you want to put the item.
    - You can add multiple items to a collection instead of adding one item at a time. To add multiple items, select the items and then drag them to a collection. Or you can select the items, right-click and then pick the collection where you want the items.
- You can add all the tabs in an Edge window into a new collection without adding them individually. To do this, right-click on any tab and choose "Add all tabs to a new collection".
- Extension sync is now available. You can now sync your extensions across all your devices! Extensions from both the Microsoft and Chrome Stores will sync with Microsoft Edge. To use this feature: Click the ellipses (...) on the menu bar, select **Settings**. Under Your profile, click **Sync** to see the Sync options. Under **Profiles/Sync** use the toggle to enable Extensions. You can use the SyncTypesListDisabled group policy to disable syncing of extensions.
- Improved the message on the Downloads management page for insecure downloads that have been blocked.
- Immersive Reader improvements:
    - Added support for Adverbs in the Parts of Speech experience we have in Immersive Reader. While reading an article within the Immersive Reader, open the Grammar Tools and switch on Adverbs

within Parts of Speech to highlight all the adverbs on the page.
    - Added the ability to select any content on a webpage and open it in Immersive Reader. This ability enables users to use the Immersive Reader and all the Learning Tools, such as Line Focus and Read Aloud, across all websites.
- Link doctor provides host correction and a search query to the users when they mistype a URL. For example:
  A user mistypes "powerbi as "powerbbi".com. Link doctor will suggest "powerbi".com as a correction and create a link to search for "powerbbi" in case the user is looking for something different.
- Allow users to save their decision to launch an external protocol for a specific site. Users can configure the ExternalProtocolDialogShowAlwaysOpenCheckbox policy to enable or disable this feature.
- Users can set Microsoft Edge as their default browser directly from Microsoft Edge **Settings**. This makes it easier for users to change their default browser, within the context of the browser itself, instead of having to search through the operating system settings. To use this feature, go to *edge://settings/defaultBrowser* and click **Make default**.
- Several DevTools updates, including new remote debugging support, UI improvements, and more. For more details, see What's New In DevTools (Microsoft Edge 83).
- Microsoft Defender for Cloud Apps warn scenario is now available. This enables admins to set up warn, a new category of Defender for Cloud Apps blocks, where the user can override a Defender for Cloud Apps block page. MDATP E5 blocks are natively integrated with SmartScreen blocks in Microsoft Edge for a seamless experience. This experience allows for a full page red block with the message "This website is blocked by your organization", instead of just a toast notification.
- Disallow synchronous XmlHttpRequest in page dismissal. Sending of synchronous XmlHttpRequests during unload of a webpage will be removed. This change improves browser performance and reliability, but may impact web applications that have not yet been updated to use more modern web APIs, including sendBeacon and fetch. The Group Policy to disable this change and permit synchronous XHR during page dismissal will be available until Microsoft Edge 88. For more information, see Site compatibility-impacting changes coming to Microsoft Edge.

Policy updates

New policies

15 new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added.

- AllowSurfGame - Allow surf game.
- AllowTokenBindingForUrls - Configure the list of sites for which Microsoft Edge will attempt to establish a Token Binding with.
- BingAdsSuppression - Block all ads on Bing search results.
- BuiltinCertificateVerifierEnabled - Determines whether the built-in certificate verifier will be used to verify server certificates.
- ClearCachedImagesAndFilesOnExit - Clear cached images and files when Microsoft Edge closes.
- ConfigureShare - Configure the Share experience.
- DeleteDataOnMigration - Delete old browser data on migration.
- DnsOverHttpsMode - Control the mode of DNS-over-HTTPS.
- DnsOverHttpsTemplates - Specify URI template of desired DNS-over-HTTPS resolver.
- FamilySafetySettingsEnabled - Allow users to configure Family safety.
- LocalProvidersEnabled - Allow suggestions from local providers.
- ScrollToTextFragmentEnabled - Enable scrolling to text specified in URL fragments.
- ScreenCaptureAllowed - Allow or deny screen capture.

- SyncTypesListDisabled - Configure the list of types that are excluded from synchronization.
- NativeWindowOcclusionEnabled - Enable Hiding of Native Windows.

Deprecated policy

The following policy will continue to work in this release. It will become "obsolete" in a future release.

EnableDomainActionsDownload Enable Domain Actions Download from Microsoft

Version 81.0.416.77: May 18

Fixed various bugs and performance issues.

Version 81.0.416.72: May 7

Security updates are listed here

Version 81.0.416.68: April 29

Security updates are listed here

Version 81.0.416.64: April 23

Security updates are listed here

Version 81.0.416.58: April 17

Security updates are listed here

Version 81.0.416.53: April 13

Security updates are listed here

Feature updates

- Added support for Windows Information Protection (WIP), which helps enterprises protect sensitive data from unauthorized disclosure. Learn More.
- Collections is now available. To get started, click the Collections icon next to the address bar. This action opens the Collections pane where you can create, edit, and view Collections. We designed Collections based on what you do on the web. If you're a shopper, a traveler, a teacher, or a student, Collections can help. Learn more.
- Allow the removal (Hide from toolbar) of the Collections button from the Microsoft Edge toolbar for consistency.
- On-prem Active Directory account auto sign in will only be targeted to organizations that turn it on. If users were already signed in with an on-prem AD account, they will be able to sign out of it. Users will only be automatically signed in with the primary account on their operating system if it's a Microsoft account or an Azure Active Directory account. Admins can enable auto sign in with an on-prem AD account using the ConfigureOnPremisesAccountAutoSignIn policy.
- Application Guard. Extensions support now available in the container.
- Added a message to inform users that Internet Explorer isn't installed when they navigate to a page that's configured to open in Internet Explorer mode.
- Updated the 3D View tool in Microsoft Edge DevTools with a new feature to help debug z-index stacking context. 3D View shows a representation of the DOM (Document Object Model) depth using color and

stacking, and the z-Index view helps you isolate the different stacking contexts of your page. Learn more.

- The F12 Dev tools are localized in 10 new languages, so they will match the language used in the rest of the browser. Learn more.
- Added support for Dolby Vision playback. On Dolby Vision-enabled Windows 10 Build 17134 (April 2018 Update), websites can show Dolby vision content. See how to enable Dolby Vision content from Netflix.
- Microsoft Edge can now identify and remove duplicate favorites and merge folders with the same name. To access the tool, click the star on the browser's toolbar and select "Remove duplicate favorites". You can that confirm changes and any updates to your favorites will be synced across devices.
- We heard from users it can be difficult to distinguish a normal browsing window in dark theme from an InPrivate window since both window frames are dark. The new solid InPrivate blue pill in the top right corner helps reassure users they are browsing InPrivate.
- Open external links in the correct browser profile. Select a default profile for links opened for external apps to open in from *edge://settings/multiProfileSettings*.
- Added a warning that alerts users who sign into a browser profile with an account after being previously signed in with another account. This warning will help prevent unintentional data merging.
- If you have payment cards saved in your Microsoft account, you can use them in Microsoft Edge while filling out payment forms. The cards in your Microsoft account will sync across desktop devices and the full details will be shared with the website after two-factor authentication (CVC code and your Microsoft identity.) For further convenience, you can choose to securely save a copy of the card on the device during authentication.
- Line Focus is designed for users who like to focus on a limited part of the content as they read. It lets users keep the focus on one, three, or five lines at a time and dims out the rest of the page to let users read without distraction. Users can scroll using touch or arrow keys and the focus shifts accordingly.
- Microsoft Edge is now integrated with Windows Speller on Windows platforms 8.1 and above. This integration provides greater language support, with access to more language dictionaries and the ability to use Windows custom dictionaries. There's no further action needed from the users when a language has been added in the OS language settings. Also, a language spellcheck toggle is enabled in Microsoft Edge settings.
- When PDF documents are opened using Microsoft Edge, users will now be able to create highlights, change color, and delete highlights. This feature helps in referencing important parts of the document later, and for collaboration.
- When loading long PDF documents that have been optimized for web, the pages being viewed by the user will be loaded faster, parallelly, while the rest of the document is loading.
- Now it's easier to start the Immersive Reader for a website by just pressing the F9 key.
- Now it's easier to start Read Aloud by using a keyboard shortcut (Ctrl + Shift + U).
- Added an MSI command line parameter that lets you suppress Desktop icon creation when you install Microsoft Edge. The following example shows how to use this new parameter:
  `MicrosoftEdgeEnterpriseX64.msi DONOTCREATEDESKTOPSHORTCUT=true`
  There will be a group policy to support this functionality in an upcoming release.

Policy updates

New policies

11 new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added.

- AmbientAuthenticationInPrivateModesEnabled - Enable Ambient Authentication for InPrivate and Guest profiles.
- AudioSandboxEnabled - Allow the audio sandbox to run.
- ForceLegacyDefaultReferrerPolicy - Use a default referrer policy of no-referrer-when-downgrade.
- GloballyScopeHTTPAuthCacheEnabled - Enable globally scoped HTTP auth cache.
- ImportExtensions - Allow importing of extensions.
- ImportCookies - Allow importing of Cookies.
- ImportShortcuts - Allow importing of shortcuts.
- InternetExplorerIntegrationSiteRedirect - Specify how "in-page" navigations to unconfigured sites behave when started from Internet Explorer mode pages.
- StricterMixedContentTreatmentEnabled - Enable stricter treatment for mixed content.
- TLS13HardeningForLocalAnchorsEnabled - Enable a TLS 1.3 security feature for local trust anchors.
- ConfigureOnPremisesAccountAutoSignIn - Configure automatic sign in with an Active Directory domain account when there is no Azure AD domain account.

Policy name and caption changes

The policy `OmniboxMSBProviderEnabled` is changed to AddressBarMicrosoftSearchInBingProviderEnabled - The caption for the policy is "Enable Microsoft Search in Bing suggestions in the address bar".

Deprecated policies

The following policies continue to work in this release. They will become "obsolete" in a future release.

- WebComponentsV0Enabled - Re-enable Web Components v0 API until M84.
- WebDriverOverridesIncompatiblePolicies - Allow WebDriver to Override Incompatible.

Resolved issues

- Fixed an issue where IE mode on Microsoft Edge caused an ongoing download dialog to show even after the file was downloaded.
- Fixed an issue where Microsoft Edge was dropping session cookies when a page already in IE mode triggered to open a new IE mode tab.

Version 80.0.361.111: April 7

Fixed various bugs and performance issues.

Version 80.0.361.109: April 1

Security updates are listed here

Version 80.0.361.69: March 19

Security updates are listed here

Version 80.0.361.66: March 4

Security updates are listed here

Version 80.0.361.62: February 25

Security updates are listed here

Version 80.0.361.57: February 20

Security updates are listed here

Version 80.0.361.56: February 19

Fixed various bugs and performance issues.

Version 80.0.361.54: February 14

Resolved issues

- Fixed an issue where Password, Payment, and Cookies fail to get imported in Microsoft Edge.

Version 80.0.361.50: February 11

Fixed various bugs and performances fixes.

Version 80.0.361.48: February 7

Security updates are listed here

Feature updates

- Added SmartScreen protection from downloading potentially unwanted apps. Learn more
- Added support for Dolby Vision playback.
- Enabled users of Windows Mixed Reality to view 360° videos on VR headsets.
- Added an option to Reading View to increase text spacing.
- Added support for erasing link using the Surface Pen eraser.
- Added support for using the arrow keys and spacebar to draw on feedback screenshots in editor mode.
- Improved the reliability of screenshots so they stop appearing all black when submitting feedback.
- Added dark theme support to the local new tab page that is shown when the device isn't connected to the internet.
- Added the ability for websites that are installed as apps to be restored when a browser session is restored after an update, crash, and so on.
- Added dark theme support to PDF UI when the browser is managed by Group Policy.
- Updated Adobe Flash to version 32.0.0.321. Learn more

Policy updates

New policies

16 new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added.

- AlternateErrorPagesEnabled - Suggest similar pages when a webpage can't be found.
- DefaultInsecureContentSetting - Control use of insecure content exceptions.
- DNSInterceptionChecksEnabled - DNS interception checks enabled.
- HideFirstRunExperience - Hide the First-run experience and splash screen.
- InsecureContentAllowedForUrls - Allow insecure content on specified sites.
- InsecureContentBlockedForUrls - Block insecure content on specified sites.
- LegacySameSiteCookieBehaviorEnabled - Enable default legacy SameSite cookie behavior setting.
- LegacySameSiteCookieBehaviorEnabledForDomainList - Revert to legacy SameSite behavior for cookies on specified sites.
- PaymentMethodQueryEnabled - Allow websites to query for available payment methods.
- PersonalizationReportingEnabled - Allow personalization of ads, search, and news by sending browsing history to Microsoft.
- PinningWizardAllowed - Allow Pin to taskbar wizard.
- SmartScreenPuaEnabled - Configure Microsoft Defender SmartScreen to block potentially unwanted apps.

- TotalMemoryLimitMb - Set limit on megabytes of memory a single Microsoft Edge instance can use.
- WebAppInstallForceList - Configure list of force-installed Web Apps.
- WebComponentsV0Enabled - Re-enable Web Components v0 API until M84.
- WebRtcLocalIpsAllowedUrls - Manage exposure of local IP addresses by WebRTC.

Deprecated policies

The following policy was deprecated.

- NewTabPageCompanyLogo - Set new tab page company logo.

Resolved issues

- Fixed an issue where audio isn't working in Citrix environment.
- Fixed an issue where Microsoft Edge and legacy Microsoft Edge side-by-side experience results in broken legacy links and crashes.

See also

- Microsoft Edge Enterprise landing page

Release notes for Microsoft Edge Beta Channel

11/1/2022 • 3 minutes to read • Edit Online

These release notes provide information about new features and non-security updates that are included in the Microsoft Edge Beta Channel. Archived versions of these release notes are available at Archived release notes for Microsoft Edge Beta Channel.

> **NOTE**
> Microsoft Edge Web Platform constantly evolves to improve user experience, security, and privacy. To learn more, see Site compatibility-impacting changes coming to Microsoft Edge.

Version 107.0.1418.23: October 26, 2022

Fixed various bugs and performance issues.

Version 107.0.1418.20: October 24, 2022

Fixed various bugs and performance issues.

Version 107.0.1418.16: October 20, 2022

Fixed various bugs and performance issues.

Version 107.0.1418.13: October 18, 2022

Fixed various bugs and performance issues.

Version 107.0.1418.8: October 13, 2022

Feature updates

- **Microsoft Edge sidebar.** The Microsoft Edge sidebar lets users access productivity tools side-by-side with their browsing window. For enterprise customers, the following experiences are currently turned on by default: Search, Discover, Office.com, and Outlook. Administrators can control the availability and configure the Microsoft Edge sidebar using the HubsSidebarEnabled, ExtensionInstallBlockList, and ExtensionInstallForceList policies. The extension ID for each sidebar app can be found at *edge://sidebar-internals*. For more information, see Manage the sidebar in Microsoft Edge.

- **New policy to give more flexibility in Microsoft Edge startup.** The RestoreOnStartupUserURLsEnabled policy lets users add and remove their own URLs to open when starting Microsoft Edge while maintaining the mandatory list of sites specified by the admin.

Policy updates

New policies

- EdgeWorkspacesEnabled - Enable Workspaces
- EnhanceSecurityModeBypassIntranet - Enhanced Security Mode configuraton for Intranet zone sites
- EventPathEnabled - Re-enable the Event.path API until Microsoft Edge version 115
- InternetExplorerIntegrationLocalMhtFileAllowed - Allow local MHTML files to open automatically in Internet Explorer mode

- LinkedAccountEnabled - Enable the linked account feature
- PerformanceDetectorEnabled - Performance Detector Enabled
- RestoreOnStartupUserURLsEnabled - Allow users to add and remove their own sites during startup when the RestoreOnStartupURLs policy is configured
- DefaultShareAdditionalOSRegionSetting - Set the default "share additional operating system region" setting
- WebSelectEnabled - Web Select Enabled
- WebSQLAccess - Force WebSQL to be enabled
- WebSQLNonSecureContextEnabled - Force WebSQL in non-secure contexts to be enabled

Deprecated policy

- MicrosoftOfficeMenuEnabled - Allow users to access the Microsoft Office menu

Obsoleted policy

- BuiltinCertificateVerifierEnabled - Determines whether the built-in certificate verifier will be used to verify server certificates

Version 106.0.1370.30: September 29, 2022

Fixed various bugs and performance issues.

Version 106.0.1370.26: September 26, 2022

Fixed various bugs and performance issues.

Version 106.0.1370.17: September 16, 2022

Fixed various bugs and performance issues.

Version 106.0.1370.15: September 15, 2022

Fixed various bugs and performance issues.

Feature updates

- **More reliable web defense.** Browse the web with more reliable protection thanks to the rewritten Microsoft Defender SmartScreen library for Microsoft Edge on Windows and macOS. The new SmartScreen library was first made available on Windows with Microsoft Edge version 103, and now makes its debut on macOS with Microsoft Edge version 106. The NewSmartScreenLibraryEnabled policy is now deprecated in Microsoft Edge version 106 and will be obsolete in Microsoft Edge version 107.

Policy updates

New policies

- EfficiencyModeEnabled - Efficiency mode enabled
- EfficiencyModeOnPowerEnabled - Enable efficiency mode when the device is connected to a power source
- InternetExplorerIntegrationAlwaysUseOSCapture Always use the OS capture engine to avoid issues with capturing Internet Explorer mode tabs

Deprecated policies

- NewSmartScreenLibraryEnabled – Allows the Microsoft Edge browser to load the new SmartScreen library for any SmartScreen checks on site URLs or application downloads.

Obsoleted policies

- OutlookHubMenuEnabled - Allow users to access the Outlook menu
- EdgeDiscoverEnabled - Discover feature In Microsoft Edge

Version 105.0.1343.34: September 9, 2022

Fixed various bugs and performance issues.

Version 105.0.1343.27: September 2, 2022

Fixed various bugs and performance issues.

Version 105.0.1343.23: August 31, 2022

Fixed various bugs and performance issues.

Version 105.0.1343.17: August 26, 2022

Fixed various bugs and performance issues.

Version 105.0.1343.10: August 19, 2022

Fixed various bugs and performance issues.

See also

- Microsoft Edge Enterprise landing page

Archived release notes for Microsoft Edge Beta Channel

11/1/2022 • 73 minutes to read • Edit Online

These release notes provide information about new features and non-security updates that are included in the Microsoft Edge Beta Channel. To understand Microsoft Edge channels, see the Overview of the Microsoft Edge channels. All the security updates are listed here.

Version 105.0.1343.7: August 16, 2022

Fixed various bugs and performance issues.

Feature updates

- **Improvement to the Cloud Site List Management experience for IE mode.**
  - You can restore to one of the last 3 published versions of your site list in the Microsoft 365 Admin Center. For more information, see Restore a previous version of a site list.
  - You can identify gaps in your enterprise site list by configuring reporting of site feedback with the InternetExplorerIntegrationCloudUserSitesReporting and InternetExplorerIntegrationCloudNeutralSitesReporting policies. You can view local site list URLs from users and potentially misconfigured neutral site URLs in the Microsoft Edge site lists experience in the Microsoft 365 Admin Center. To learn more, see View site feedback on the Microsoft 365 Admin Center.
  - You can configure session cookie sharing between Microsoft Edge and Internet Explorer for IE mode on your site list in the Microsoft 365 Admin Center. To learn more, see Cookie sharing between Microsoft Edge and Internet Explorer.
- **Improvements to the Cloud Site List Management experience for IE mode now available in GCC.** GCC customers can now utilize the full Microsoft Edge site list experience in the Microsoft 365 Admin Center.

Policy updates

New policies

- ExemptFileTypeDownloadWarnings - Disable download file type extension-based warnings for specified file types on domains
- InternetExplorerIntegrationAlwaysWaitForUnload - Wait for Internet Explorer mode tabs to completely unload before ending the browser session
- MicrosoftEditorProofingEnabled - Spell checking provided by Microsoft Editor
- MicrosoftEditorSynonymsEnabled - Synonyms are provided when using Microsoft Editor spell checker
- PrintPdfAsImageDefault - Print PDF as Image Default
- UnthrottledNestedTimeoutEnabled - JavaScript setTimeout will not be clamped until a higher nesting threshold is set

Deprecated policy

- ExemptDomainFileTypePairsFromFileTypeDownloadWarnings - Disable download file type extension-based warnings for specified file types on domains

Additional change

- GuidedSwitchEnabled - Add Linux platform support

Version 104.0.1293.44: August 3

Fixed various bugs and performance issues.

Feature updates

- **Enhance your security on the web**. Improvements to **Enhance your security on the web** in *edge://settings/privacy* now include **Basic** as the new default option. With this option, Microsoft Edge will apply added security protection to the less visited sites. This preserves the user experience for the most popular sites on the web. For more information, see Browse more safely with Microsoft Edge.

Version 104.0.1293.41: August 1

Fixed various bugs and performance issues.

Version 104.0.1293.35: July 25

Fixed various bugs and performance issues.

Version 104.0.1293.25: July 18

Fixed various bugs and performance issues.

Feature updates

- **Import Chrome data without Chrome during First Run Experience.** This feature lets a user bring in their Chrome data by logging in to their Google account during Microsoft Edge's First Run Experience. This feature can be turned off by disabling First Run Experience with the HideFirstRunExperience policy, or by setting AutoImportAtFirstRun to 'DisabledAutoImport'.

Version 104.0.1293.21: July 14

Fixed various bugs and performance issues.

Version 104.0.1293.14: July 7

Policy updates

New policies

- AllowedDomainsForApps - Define domains allowed to access Google Workspace
- AskBeforeCloseEnabled - Get user confirmation before closing a browser window with multiple tabs
- BrowserCodeIntegritySetting - Configure browser process code integrity guard setting
- DoubleClickCloseTabEnabled - Double Click feature in Microsoft Edge enabled (only available in China)
- ImportOnEachLaunch - Allow import of data from other browsers on each Microsoft Edge launch
- QuickSearchShowMiniMenu - Enables Microsoft Edge mini menu
- PasswordManagerRestrictLengthEnabled - Restrict the length of passwords that can be saved in the Password Manager
- PDFXFAEnabled - XFA support in native PDF reader enabled
- TextPredictionEnabled - Text prediction enabled by default

Obsoleted policy

- U2fSecurityKeyApiEnabled - Allow using the deprecated U2F Security Key API

Version 103.0.1264.45: July 1

Fixed various bugs and performance issues.

Version 103.0.1264.37: June 22

Fixed various bugs and performance issues.

Version 103.0.1264.32: June 20

Fixed various bugs and performance issues.

Version 103.0.1264.21: June 10

Fixed various bugs and performance issues.

Version 103.0.1264.17: June 6

Fixed various bugs and performance issues.

Version 103.0.1264.13: June 2

Feature updates

- **Ability to control automatic profile switching.** The GuidedSwitchEnabled policy lets Microsoft Edge prompt the user to switch to the appropriate profile when Microsoft Edge detects that a link is a personal or work link.
- **Client Certificate Switcher.** This feature will offer a way for users to clear the remembered certificate and resurface the certificate picker when visiting a site requiring http certificate authentication. Switching can be done without manually quitting Microsoft Edge.
- **More reliable web defense.** Browse the web with more reliable protection thanks to the rewritten Microsoft Defender SmartScreen library for Microsoft Edge on Windows. The NewSmartScreenLibraryEnabled policy will allow enterprise customers to continue using the legacy version of the library until it's deprecated in Microsoft Edge version 105.

Policy updates

New policies

- GuidedSwitchEnabled - Guided Switch Enabled
- InternetExplorerZoomDisplay - Display zoom in IE Mode tabs with DPI Scale included like it is in Internet Explorer
- LiveCaptionsAllowed - Live captions allowed
- OriginAgentClusterDefaultEnabled - Origin-keyed agent clustering enabled by default

Version 102.0.1245.25: May 26

Fixed various bugs and performance issues.

Version 102.0.1245.22: May 24

Fixed various bugs and performance issues.

Version 102.0.1245.18: May 20

Fixed various bugs and performance issues.

Version 102.0.1245.14: May 16

Fixed various bugs and performance issues.

Version 102.0.1245.12: May 13

Fixed various bugs and performance issues.

Version 102.0.1245.7: May 10

Policy updates

New policies

- AllHttpAuthSchemesAllowedForOrigins - List of origins that allow all HTTP authentication
- OutlookHubMenuEnabled - Allow users to access the Outlook menu
- NetworkServiceSandboxEnabled - Enable the network service sandbox
- UserAgentClientHintsGREASEUpdateEnabled - Control the User-Agent Client Hints GREASE Update feature

Version 101.0.1210.39: May 5

Fixed various bugs and performance issues.

Version 101.0.1210.31: April 27

Fixed various bugs and performance issues.

Version 101.0.1210.26: April 22

Fixed various bugs and performance issues.

Version 101.0.1210.19: April 18

Fixed various bugs and performance issues.

Version 101.0.1210.14: April 12

Fixed various bugs and performance issues.

Feature updates

- **Improvements to the Enterprise Site List Manager.** Now you can configure shared cookies between Microsoft Edge and Internet Explorer on your enterprise site list. You can access the Enterprise Site List Manager at *edge://compat/SiteListManager*.

Version 101.0.1210.10: April 8

Feature updates

- **Ability to set default profile.** The EdgeDefaultProfileEnabled policy will let you set a default profile to be used when opening the browser rather than the last profile used. This policy won't be applicable if the `--profile-directory` parameter has been specified.
- **Launch Progressive Web Apps (PWAs) from Favorites Bar.** Improvements to the PWA launch experience will begin to show up starting with an Apps icon that can be added to the toolbar.
- **Manage the "Allow extensions from other stores" setting.** Use the ControlDefaultStateOfAllowExtensionFromOtherStoresSettingEnabled policy to control the default state of the "Allow extensions from other stores" setting.

Policy updates

New policies

- ConfigureKeyboardShortcuts - Configure the list of commands for which to disable keyboard shortcuts
- ControlDefaultStateOfAllowExtensionFromOtherStoresSettingEnabled - Configure default state of Allow extensions from other stores setting
- EdgeAssetDeliveryServiceEnabled - Allow features to download assets from the Asset Delivery Service
- EdgeDefaultProfileEnabled - Default Profile Setting Enabled
- InternetExplorerModeEnableSavePageAs - Allow Save page as in Internet Explorer mode
- KioskSwipeGesturesEnabled - Swipe gestures in Microsoft Edge kiosk mode enabled
- MicrosoftOfficeMenuEnabled - Allow users to access the Microsoft Office menu
- SiteSafetyServicesEnabled - Allow users to configure Site safety services

Deprecated policy

- ForceCertificatePromptsOnMultipleMatches - Configure whether Microsoft Edge should automatically select a certificate when there are multiple certificate matches for a site configured with "AutoSelectCertificateForUrls"

Obsoleted policy

- WebSQLInThirdPartyContextEnabled - Force WebSQL in third-party contexts to be re-enabled

Version 100.0.1185.27: March 31

Fixed various bugs and performance issues.

Version 100.0.1185.23: March 28

Fixed various bugs and performance issues.

Version 100.0.1185.17: March 23

Fixed various bugs and performance issues.

Version 100.0.1185.12: March 18

Fixed various bugs and performance issues.

Feature updates

- **Streamlining Microsoft 365 Application Protocol Activations.** Microsoft 365 Application Protocol Activations on trusted Microsoft cloud storage services will now launch certain Microsoft 365 applications directly, including SharePoint subdomains and Microsoft OneDrive URLs. You can use the policies AutoLaunchProtocolsComponentEnabled and AutoLaunchProtocolsFromOrigins to enable the application protocol activation prompts if desired, and to define other applications and services where warnings are enabled or disabled.

Version 100.0.1185.10: March 17

Feature updates

- **Improvements to the Cloud Site List Management experience for IE Mode.** You can configure session cookie sharing between Microsoft Edge and Internet Explorer for IE Mode on your site list in the Microsoft 365 Admin Center. **Note:** This is a controlled feature rollout. If you don't see this feature, check back as we continue our rollout

- **Preview PDF files in Microsoft Outlook and File Explorer.** Users can view a PDF file in a

lightweight and rich read-onlypreview. Available for Outlook Desktop PDF attachments or for local PDF files using File Explorer.

- **Installed web app synchronization across all desktop devices.** Websites or Progressive Web Apps (PWAs) that have been installed as applications will synchronize across all desktop devices that you've signed into and enabled sync on. They'll show as "Available apps" for you to install. An app removed from one device will sync the removal on all devices.

Policy updates

New policies

- AdsTransparencyEnabled - Configure if the ads transparency feature is enabled
- DefaultWebHidGuardSetting - Control use of the WebHID API
- HideRestoreDialogEnabled - Hide restore pages dialog after browser crash
- PDFSecureMode - Secure mode and Certificate-based Digital Signature validation in native PDF reader
- PromptOnMultipleMatchingCertificates - Prompt the user to select a certificate when multiple certificates match
- WebHidAskForUrls - Allow the WebHID API on these sites
- WebHidBlockedForUrls - Block the WebHID API on these sites

Deprecated policy

- BackgroundTemplateListUpdatesEnabled - Enables background updates to the list of available templates for Collections and other features that use templates

Obsoleted policy

- AllowSyncXHRInPageDismissal - Allow pages to send synchronous XHR requests during page dismissal

Version 99.0.1150.39: March 10

Feature updates

- **Improvements to the Cloud Site List Management experience for IE Mode.** Identify gaps in your enterprise site list by configuring reporting of site feedback with the InternetExplorerIntegrationCloudUserSitesReporting and InternetExplorerIntegrationCloudNeutralSitesReporting policies. You can view local site list URLs from users and potentially misconfigured neutral site URLs in the Microsoft Edge site lists experience in the Microsoft 365 Admin Center. To learn more, see View site feedback on the Microsoft 365 Admin Center. **Note:** This is a controlled feature rollout. If you don't see this feature, check back as we continue our rollout.

Version 99.0.1150.30: March 2

Fixed various bugs and performance issues.

Version 99.0.1150.25: February 25

Fixed various bugs and performance issues.

Version 99.0.1150.21: February 22

Fixed various bugs and performance issues.

Version 99.0.1150.16: February 14

Fixed various bugs and performance issues.

Version 99.0.1150.11: February 9

Feature updates

- **Upcoming three-digit version number in user agent string.** Starting with version 100, Microsoft Edge will send a three-digit version number in the User-Agent header, for example "Edg/100". Starting with Microsoft Edge 97, site owners can test this upcoming agent string by enabling the **#force-major-version-to-100** experiment flag in *edge://flags* to ensure their User-Agent parsing logic is robust and works as expected.
- **Personalize multi-profile experiences with profile preferences for sites.** Users can personalize their multi-profile experience with the ability to create a customized list of sites for automatic profile switching in Microsoft Edge.
- **Bidirectional Cookie Sharing for IE mode.** This feature expands on the cookie sharing capability already available and lets users sync specific session cookies from Internet Explorer/IE mode to Microsoft Edge. For more information, see Cookie sharing between Microsoft Edge and Internet Explorer.
- **Navigate PDF documents using page thumbnails.** You will now be able to navigate through your PDF document using thumbnails that represent the pages. These thumbnails will appear in the pane on the left side of the PDF reader.
- **Configure the list of domains for which the password manager User Interface (UI) for Save and Fill will be disabled.** Use the PasswordManagerBlocklist policy to configure the list of domains (HTTP/HTTPS schemas and hostnames only) where Microsoft Edge should disable the password manager. This means that Save and Fill workflows will be disabled, which ensures that passwords for those websites can't be saved or auto filled into web forms.
- **Update extensions to the Microsoft Edge Add-ons store using API's (in public preview).** You can integrate these API's directly into your build pipeline, and publish package updates to the Microsoft Edge Add-on website. To learn more, see Using the Microsoft Edge Add-ons API (in private preview)

Policy updates

New policies

- AllowGamesMenu - Allow users to access the games menu
- DoNotSilentlyBlockProtocolsFromOrigins - Define a list of protocols that can not be silently blocked by anti-flood protection
- HubsSidebarEnabled - Show Hubs Sidebar
- InternetExplorerIntegrationCloudNeutralSitesReporting - Configure reporting of potentially misconfigured neutral site URLs to the M365 Admin Center Site Lists app
- InternetExplorerIntegrationCloudUserSitesReporting - Configure reporting of IE Mode user list entries to the M365 Admin Center Site Lists app
- PasswordManagerBlocklist - Configure the list of domains for which the password manager UI (Save and Fill) will be disabled
- RelatedMatchesCloudServiceEnabled - Configure Related Matches in Find on Page
- SignInCtaOnNtpEnabled - Enable sign in click to action dialog
- UserAgentReduction - Enable or disable the User-Agent Reduction

Version 98.0.1108.48: February 8

Fixed various bugs and performance issues.

Version 98.0.1108.43: February 3

Fixed various bugs and performance issues.

Version 98.0.1108.42: February 2

Fixed various bugs and performance issues.

Version 98.0.1108.39: January 31

Fixed various bugs and performance issues.

Version 98.0.1108.33: January 24

Fixed various bugs and performance issues.

Version 98.0.1108.27: January 19

Fixed various bugs and performance issues.

Version 98.0.1108.23: January 14

Feature updates

- **Enhance your security on the web.** A browsing mode in Microsoft Edge where the security of your browser takes priority, giving you an extra layer of protection when browsing the web. Administrators can apply the following Group Policies to end-user desktops (Windows, macOS, and Linux) to help protect against zero days. These policies also make that important sites and line of business applications continue to work as expected. This feature is a huge step forward because it lets us mitigate unforeseen active zero days (based on historical trends). When turned on, this feature brings Hardware-enforced Stack Protection, Arbitrary Code Guard (ACG), and Content Flow Guard (CFG) as supporting security mitigations to increase users' security on the web. Group Policies:
    - EnhanceSecurityMode
    - EnhanceSecurityModeBypassListDomains
    - EnhanceSecurityModeEnforceListDomains
- **Custom primary password.** The browser already has the capability where users can add an authentication step before saved passwords are auto-filled in web forms. This adds another layer of privacy and helps prevent unauthorized users from using saved passwords to log on websites. Custom primary password is an evolution of that same feature, where users will now be able to use a custom string of their choice as their primary password. After it's enabled, users will enter this password to authenticate themselves and have their saved passwords auto filled into web forms.
- **Overlay scrollbars added to Microsoft Edge.** We've updated our scrollbars with an overlay-based design. Users can turn this feature on in *edge://flags*.

Policy updates

New Policies

- AddressBarEditingEnabled - Configure address bar editing.
- EdgeFollowEnabled - Enable Follow service in Microsoft Edge.
- EnhanceSecurityMode - Enhance the security state in Microsoft Edge.
- EnhanceSecurityModeBypassListDomains - Configure the list of domains for which enhance security mode will not be enforced.
- EnhanceSecurityModeEnforceListDomains - Configure the list of domains for which enhance security mode will always be enforced.
- InAppSupportEnabled - In-app support Enabled.
- MicrosoftEdgeInsiderPromotionEnabled - Microsoft Edge Insider Promotion Enabled.
- PrintStickySettings - Print preview sticky settings.

- SandboxExternalProtocolBlocked - Allow Microsoft Edge to block navigations to external protocols in a sandboxed iframe.
- U2fSecurityKeyApiEnabled - Allow using the deprecated U2F Security Key API.

Version 97.0.1072.54: January 5

Fixed various bugs and performance issues.

Version 97.0.1072.52: January 3

Fixed various bugs and performance issues.

Version 97.0.1072.41: December 20

Fixed various bugs and performance issues.

Version 97.0.1072.34: December 13

Fixed various bugs and performance issues.

Version 97.0.1072.28: December 8

Fixed various bugs and performance issues.

Version 97.0.1072.21: December 1

Feature updates

- **Use current profile to sign into websites when multiple work or school accounts are signed in on a device.** When multiple work or school accounts are signed in on a device, users will be asked to choose an account from the account picker to continue their visits to websites. In this release, users will be prompted to allow Microsoft Edge to sign in to the websites automatically with the work and school account that's signed into current profile. Users can turn this feature on and off in **Settings/Profile preferences**.
- **Add support for Microsoft Endpoint Data Loss Prevention (DLP) on macOS.** Microsoft Endpoint DLP policy enforcement is available natively on macOS.
- **Open digitally signed PDF files.** Digital signatures are used extensively to validate the authenticity of, and changes to, a document. Users can validate the signatures for PDF files directly from the browser, without the need for any add-ins.
- **Citations in Microsoft Edge.** Citing sources for research is a common requirement for students. They have to manage many research references and sources, which aren't easy tasks. They also have to translate these citations to proper citation formats like APA, MLA, and Chicago. This new "Citations" feature in Microsoft Edge (now in Preview) gives students a better way to manage and generate citations as they research online. With Citations turned on in Collections or from **Settings and more (Alt-F)**, Microsoft Edge automatically generates citations that students can use later so they can stay focused on their research. When they're done, they can easily compile these citations into a final deliverable. For more information, see Previewing Citations in Microsoft Edge.

Policy updates

New Policies

- AccessibilityImageLabelsEnabled - Get Image Descriptions from Microsoft Enabled
- CORSNonWildcardRequestHeadersSupport - CORS non-wildcard request header support enabled

- EdgeDiscoverEnabled - Discover feature In Microsoft Edge
- EdgeEnhanceImagesEnabled - Enhance images enabled
- InternetExplorerModeTabInEdgeModeAllowed - Allow sites configured for Internet Explorer mode to open in Microsoft Edge
- SameOriginTabCaptureAllowedByOrigins - Allow Same Origin Tab capture by these origins
- ScreenCaptureAllowedByOrigins - Allow Desktop, Window, and Tab capture by these origins
- SerialAllowAllPortsForUrls - Automatically grant sites permission to connect all serial ports
- SerialAllowUsbDevicesForUrls - Automatically grant sites permission to connect to USB serial devices
- SmartScreenDnsRequestsEnabled - Enable Microsoft Defender SmartScreen DNS requests
- TabCaptureAllowedByOrigins - Allow Tab capture by these origins
- WebSQLInThirdPartyContextEnabled - Force WebSQL in third-party contexts to be re-enabled
- WindowCaptureAllowedByOrigins - Allow Window and Tab capture by these origins

Obsoleted Policies

- AppCacheForceEnabled - Allows the AppCache feature to be re-enabled, even if it's turned off by default.

Version 96.0.1054.34: November 23

Fixed various bugs and performance issues.

Version 96.0.1054.26: November 17

Fixed various bugs and performance issues.

Version 96.0.1054.24: November 16

Fixed various bugs and performance issues.

Version 96.0.1054.13: November 5

Fixed various bugs and performance issues.

Version 96.0.1054.8: November 1

Feature updates

- **Launch Progressive Web App (PWA) directly via protocol links.** Let installed PWAs handle links that use a specific protocol for a more integrated experience.
- **Learn how to solve math problems with Math Solver.** We're excited to announce that you can use Math Solver in Microsoft Edge to get help with a wide range of mathematical concepts. These concepts range from elementary arithmetic and quadratic equations to trigonometry and calculus. Math Solver lets you take a picture of a handwritten or printed math problem and then provides an instant solution with step-by-step instructions to help you learn how to reach the solution without help. Math Solver also comes with a mathematical keyboard that you can use to easily type math problems. This keyboard eliminates the need to search around a traditional keyboard to find the math characters you need. After solving your problem, Math Solver provides options to continue learning with quizzes, worksheets, and video tutorials.
- **Freeform highlighting on PDFs.** The PDF viewing and markup experience is improved with the addition of freeform highlighters. You can highlight sections in PDFs that you don't have access to, and scanned documents.
- **Hardware-enforced Stack Protection.** Microsoft Edge will begin supporting an even safer browsing

mode that uses hardware-dependent control flow for browser processes on supported hardware (Intel 11th Gen. or AMD Zen 3). Note: Because this is a Controlled Feature Rollout you may not notice this feature enabled on all devices. You can enable or disable Hardware-enforced Stack Protection by manipulating Image File Execution Options (IFEO) using group policy.

- **New warning dialog for typosquatting sites.** The browser will now show a warning on some sites with URLs that look similar to other sites. This UI uses client-side heuristics to warn users about sites that might be spoofing popular web sites. For more information, see What is typosquatting?.
- **Improved handoff between IE mode and the modern browser.** Starting with this version of Microsoft Edge, navigations between Microsoft Edge and Internet Explorer mode will include form data and additional HTTP headers. Referrer headers, post data, forms data, and request methods will be forwarded correctly across the two experiences. You can specify which data types should be included using the InternetExplorerIntegrationComplexNavDataTypes policy. For more information, see this FAQ: My application requires transferring POST data between IE mode and Microsoft Edge.
- **Cloud Site List Management for IE mode in Public Preview.** Cloud Site List Management lets you manage your site lists for IE mode in the cloud without needing an on-premises infrastructure to host your organization's site list. You can access the Cloud Site List Management feature using the Microsoft Edge Site Lists experience in the Microsoft 365 Admin Center. To learn more, see the Cloud Site List Management for IE mode (Public Preview) article.
- **Update Microsoft Edge WebWiew2 using WSUS.** IT Admins using WSUS to update Microsoft Edge will also be able to update Microsoft Edge WebView2 using WSUS. This capability gives admins an easier servicing process for offline devices.
- **WSUS updates for Server.** WSUS and Catalog updates for Microsoft Edge channels (Stable, Beta, Dev) will now apply to Windows Server SKUs that have Microsoft Edge installed, including Windows Server 2022. For more information on how to configure WSUS updates for Microsoft Edge, see Update Microsoft Edge.

Policy updates

New Policies

- ApplicationGuardUploadBlockingEnabled - Prevents files from being uploaded while in Application Guard.
- AudioProcessHighPriorityEnabled - Allow the audio process to run with priority above normal on Windows.
- AutoLaunchProtocolsComponentEnabled - AutoLaunch Protocols Component Enabled.
- EfficiencyMode - Configure when efficiency mode should become active.
- ForceSyncTypes - Configure the list of types that are included for synchronization.
- InternetExplorerIntegrationComplexNavDataTypes - Configure whether form data and HTTP headers will be sent when entering or exiting Internet Explorer mode.
- InternetExplorerModeToolbarButtonEnabled - Show the Reload in Internet Explorer mode button in the toolbar.
- PrintPostScriptMode - Print in PostScript Mode.
- PrintRasterizePdfDpi - Print in Rasterize PDF DPI.
- RendererAppContainerEnabled - Enable renderer in app container.
- SharedLinksEnabled - Show links shared from Microsoft 365 apps in History.
- TyposquattingCheckerEnabled - Configure Edge TyposquattingChecker.

Version 95.0.1020.38: October 28

Fixed various bugs and performance issues.

Version 95.0.1020.20: October 11

Fixed various bugs and performance issues.

Version 95.0.1020.14: October 5

Fixed various bugs and performance issues.

Version 95.0.1020.9: September 28

Feature updates

- **View in File Explorer support for SharePoint Online libraries in Microsoft Edge.** Now you can enable the View in File Explorer capability for SharePoint Online Modern Document Libraries. For this experience to be visible and work for your users, you will need to enable the Microsoft Edge "Configure the View in File Explorer feature for SharePoint pages in Microsoft Edge" policy and update your SharePoint Online tenant configuration. Learn more: View SharePoint files with File Explorer in Microsoft Edge - SharePoint in Microsoft 365 | Microsoft Docs.
- **Intranet zone file URL links will open in Windows File Explorer.** You can allow file URL links to intranet zone files originating from intranet zone HTTPS websites to open Windows File Explorer for that file or directory. You can enable this experience using the IntranetFileLinksEnabled policy.
- **Improvements to the downloads experience.** Support for the download user experience is being extended to progressive web applications PWAs and WebView. We will also begin to support drag and drop to the File Explorer and Desktop.
- **Pick up where you left off on PDF documents.** You can resume reading from the location where you last closed your PDF document.
- **Efficiency mode extends battery life when your laptop enters battery saver mode.** Efficiency mode will become active when your laptop enters battery saver mode to allow the browser to manage resource usage to extend the battery life of your machine. You will have four options for when efficiency mode becomes active, Unplugged and low battery, Unplugged, Always, and Never. Note: This is a Controlled Feature Rollout. Devices with a battery should have the feature turned on.

New Policies

- BrowserLegacyExtensionPointsBlockingEnabled - Enable browser legacy extension point blocking.
- CrossOriginWebAssemblyModuleSharingEnabled - Specifies whether WebAssembly modules can be sent cross-origin.
- DisplayCapturePermissionsPolicyEnabled - Specifies whether the display-capture permissions-policy is checked or skipped.
- InternetExplorerIntegrationWindowOpenHeightAdjustment - Configure the pixel adjustment between window.open heights sourced from IE mode pages vs. Microsoft Edge mode pages.
- InternetExplorerIntegrationWindowOpenWidthAdjustment - Configure the pixel adjustment between window.open widths sourced from IE mode pages vs. Microsoft Edge mode pages.
- IntranetFileLinksEnabled - Allow intranet zone file URL links from Microsoft Edge to open in Windows File Explorer.
- ShadowStackCrashRollbackBehavior - Configure ShadowStack crash rollback behavior.
- VisualSearchEnabled - Enable visual search.

Obsoleted Policies

- InternetExplorerIntegrationTestingAllowed - Allow Internet Explorer mode testing.
- LegacySameSiteCookieBehaviorEnabled - Enable default legacy SameSite cookie behavior setting.

Version 94.0.992.23: September 17

Fixed various bugs and performance issues.

Version 94.0.992.19: September 13

Fixed various bugs and performance issues.

Version 94.0.992.14: September 7

Fixed various bugs and performance issues.

Version 94.0.992.9: September 2

Feature updates

- **Microsoft Edge moving to a 4-week cadence for updates in Beta and Stable channels.** We will adopt a new, 4-week release cycle for major versions. You can read more about the decision here: https://blogs.windows.com/msedgedev/2021/03/12/new-release-cycles-microsoft-edge-extended-stable/
- **New Extended stable option being offered.** We are offering a new Extended Stable option to our managed Enterprise customers. The Extended Stable option will stay on even numbered revisions and update every 8 weeks. There will be a biweekly security update. Additional information here: https://blogs.windows.com/msedgedev/2021/07/15/opt-in-extended-stable-release-cycle/
- **Improvements to default behavior of opening MHTML files.** MHTML files will continue to open in IE mode if IE mode is enabled, unless the MHTML file was saved from Microsoft Edge (using the Save As or Save Page As options in Microsoft Edge). If the file was saved from Microsoft Edge, it will now open in Microsoft Edge. This change will fix a rendering issue that was observed when opening an MHTML file in IE mode when saved from Microsoft Edge.
- **Restrict private network requests to secure contexts.** Access to resources on local (intranet) networks from pages on the internet requires that those pages be delivered over HTTPS. This change is happening in the Chromium project, on which Microsoft Edge is based. For more information, navigate to the Chrome Platform Status entry. Two compatibility policies are available to support scenarios that need to preserve compatibility with non-secure pages: InsecurePrivateNetworkRequestAllowed and InsecurePrivateNetworkRequestAllowedForUrls.
- **Block mixed content downloads.** Secure pages will only download files hosted on other secure pages, and downloads hosted on non-secure (non-HTTPS) pages will be blocked if initiated from a secure page. This change is happening in the Chromium project, on which Microsoft Edge is based. For more information, navigate to the Google security blog entry.
- **Enable implicit sign-in for on-premises accounts.** By enabling the OnlyOnPremisesImplicitSigninEnabled policy, only on-premises accounts will be enabled for implicit sign-in. Microsoft Edge won't attempt to implicitly sign in to MSA or AAD accounts. Upgrade from on-premises accounts to AAD accounts will be stopped as well.
- **Free form text boxes added to PDF documents.** We now support adding free form text boxes to PDF documents that you can use to fill in forms and add visible notes.
- **Update your passwords with ease.** The browser will now take you directly to the Change Password page for a given website saving you time and clicks by avoiding the need to navigate to the page manually. Once you're on this page the browser will also autofill your existing password and suggest a strong, unique new password. Please note: currently this feature is available on a limited number of sites.

- **New accessibility settings page.** We have brought accessibility-related settings together on a single page. You can find the new edge://settings/accessibility page under the main settings list. Here you can find settings to make the web page bigger, show a high visibility outline around the area of focus and other settings that can help improve your web browsing experience. We'll continue to add new settings here in future versions of Microsoft Edge.

New Policies

- ApplicationGuardPassiveModeEnabled Ignore Application Guard site list configuration and browse Edge normally
- OnlyOnPremisesImplicitSigninEnabled Only on-premises account enabled for implicit sign-in
- WebRtcRespectOsRoutingTableEnabled Enable support for Windows OS routing table rules when making peer to peer connections via WebRTC

Obsoleted Policy

- UserAgentClientHintsEnabled Enable the User-Agent Client Hints feature

Version 93.0.961.33: August 27

Fixed various bugs and performance issues.

Version 93.0.961.27: August 20

Fixed various bugs and performance issues.

Version 93.0.961.24: August 18

Fixed various bugs and performance issues.

Version 93.0.961.11: August 3

Feature updates

- **Initial Preferences in Microsoft Edge.** Starting with Microsoft Edge version 93, deploying Microsoft Edge to your enterprise will become easier with the addition of Initial Preferences.
- **IE mode on Microsoft Edge will support "no-merge" behavior.** Starting with Microsoft Edge version 93, IE mode on Microsoft Edge will support "no-merge". For an end user, when a new browser window is launched from an IE mode application, it will be in a separate session, similar to the behavior in IE11. You will need to adjust your site list to configure sites that need to prevent session sharing. Behind the scenes, for each window of Microsoft Edge, the first time an IE mode tab is visited within that window, if it is one of the designated "no-merge" sites, that window is locked into a different "no-merge" IE session from all other Microsoft Edge windows at least until the last IE mode tab is closed in that window. Learn more here.
- **Tab Groups.** The ability to categorize tabs into user-defined groups helps you more effectively find, switch, and manage tabs across multiple workstreams. To enable this, we are turning on tab grouping beginning with Microsoft Edge version 93.
- **Hide the title bar while using Vertical Tabs.** Get the extra few pixels back by hiding the browser's title bar, while in Vertical Tabs. Starting with Microsoft Edge version 93, you can go to edge://settings/appearance and under the Customize Toolbar section select the option to hide the title bar while in Vertical Tab mode.
- **Video Picture in Picture (PiP) from hover toolbar.** Starting with Microsoft Edge version 93, it will become even easier to enter Picture in Picture (PiP) mode. When you hover over a supported video, a

toolbar will appear that allows you to view that video in a PiP window. Note: this is currently available for Microsoft Edge users on macOS. Check back shortly as we continue our rollout to Windows users.

- **Removal of 3DES in TLS.** Starting with Microsoft Edge version 93, support for the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher suite will be removed. This change is happening in the Chromium project, on which Microsoft Edge is based. For more information, navigate to the Chrome Platform Status entry. Additionally, in Microsoft Edge version 93, the TripleDESEnabled policy will be available to support scenarios that need to preserve compatibility with outdated servers. This compatibility policy will become obsolete and stop working in Microsoft Edge version 95. Ensure that you update affected servers before then.

- **Policies to bypass ClickOnce and DirectInvoke prompts.** We have updated our policies to enable bypassing ClickOnce's prompts and DirectInvoke's app for specified file types, from specified domains. To do this, you will need to:

  - Enable ClickOnceEnabled or DirectInvokeEnabled
  - Enable AutoOpenFileTypes policy and set the list of specific file types that ClickOnce and DirectInvoke should be disabled for
  - Enable the AutoOpenAllowedForURLs policy and set the list of specific domains that ClickOnce and DirectInvoke will be disabled for

  Note: AutoOpenAllowedForURLs is a supporter policy for AutoOpenFileTypes. If AutoOpenAllowedForURLs is not set and AutoOpenFileTypes is set, then file types listed will automatically open from all URLs.

New Policies

- AutoplayAllowlist Allow media autoplay on specific sites
- CECPQ2Enabled CECPQ2 post-quantum key-agreement enabled for TLS
- ConfigureViewInFileExplorer Configure the View in File Explorer feature for SharePoint pages in Microsoft Edge
- DefaultJavaScriptJitSetting Control use of JavaScript JIT
- ShowPDFDefaultRecommendationsEnabled Allow notifications to set Microsoft Edge as default PDF reader
- FeatureFlagOverridesControl Configure users ability to override feature flags
- ImplicitSignInEnabled Enable implicit sign-in
- InternetExplorerIntegrationCloudSiteList Configure the Enterprise Mode Cloud Site List
- InternetExplorerIntegrationSiteListRefreshInterval Configure how frequently the Enterprise Mode Site List is refreshed
- JavaScriptJitAllowedForSites Allow JavaScript to use JIT on these sites
- JavaScriptJitBlockedForSites Block JavaScript from using JIT on these sites
- LocalBrowserDataShareEnabled Enable Windows to search local Microsoft Edge browsing data
- MAUEnabled Always use Microsoft AutoUpdate as the updater for Microsoft Edge
- MSAWebSiteSSOUsingThisProfileAllowed Allow single sign-on for Microsoft sites using this profile
- OneAuthAuthenticationEnforced OneAuth Authentication Flow Enforced for signin
- PasswordGeneratorEnabled Allow users to get a strong password suggestion whenever they are creating an account online
- PrimaryPasswordSetting Configures a setting that asks users to enter their device password while using password autofill
- PrintingWebpageLayout Sets layout for printing
- RemoteDebuggingAllowed Allow remote debugging
- RelaunchWindow Set the time interval for relaunch
- TravelAssistanceEnabled Enable travel assistance

- TripleDESEnabled Enable 3DES cipher suites in TLS

Deprecated Policy

- LegacySameSiteCookieBehaviorEnabled Enable default legacy SameSite cookie behavior setting

Obsoleted Policy

- NewTabPageSetFeedType Configure the Microsoft Edge new tab page experience

Additional Change

- ConfigureShare Add mac platform support

Version 93.0.961.18: August 10

Fixed various bugs and performance issues.

Version 92.0.902.62: July 29

Fixed various bugs and performance issues.

Version 92.0.902.55: July 21

Fixed various bugs and performance issues.

Version 92.0.902.45: July 12

Fixed various bugs and performance issues.

Version 92.0.902.40: July 6

Fixed various bugs and performance issues.

Version 92.0.902.22: June 21

Feature updates

- **Natural language search for browser history on the address bar**. Finding the article/website you are looking for is now easier thanks to natural language search right from the address bar. You can find search results based on page content/description/timing (such as "cake recipe from last week") in addition to titles/URL keyword matches alone. Please note: this is a Controlled Feature Rollout. If you don't see this feature, please check back shortly as we continue our rollout.

- **Users can easily get to Internet Explorer mode on Microsoft Edge**. Starting with Microsoft Edge version 92, users can reload a site in Internet Explorer mode on Microsoft Edge instead of relying on the standalone IE 11 application while waiting for a site to be configured in the Enterprise Mode Site List. Users will be prompted to add the site to their local site list such that navigating to the same page in Microsoft Edge will automatically render in IE mode for the next 30 days. You can use the *InternetExplorerIntegrationReloadInIEModeAllowed* policy to configure this experience and allow access to the IE mode entry points as well as the ability to add sites to the local site list. You can use the *InternetExplorerIntegrationLocalSiteListExpirationDays* policy to adjust the number of days to keep sites on the local site list. Note that KB5003698 or later is required for Windows 10, version 1909; or KB5003690 or later is required for Windows 10, version 2004, Windows 10, version 20H2, or Windows 10, version 21H1 for the end-to-end experience.

- **MHTML files will default to opening in Internet Explorer mode**. Starting in Microsoft Edge version 92 Stable, MHTML file types will automatically open in Internet Explorer mode on Microsoft Edge instead of the Internet Explorer (IE11) application. This is most commonly observed while trying to view

Outlook emails in a browser. This change will occur only if IE11 is the default handler for this file type. If you'd prefer to change this, you can do so prior to installing the Stable version 92 update using this guidance.

- **Payment instruments are now synced across devices**. Beginning with Microsoft Edge version 92, you have the option to synchronize your payment information across your signed in devices. Please note: this is a Controlled Feature Rollout. If you don't see this feature, check back shortly as we continue our rollout.
- **"Disable developer mode extensions" warning can be permanently dismissed**. Beginning with Microsoft Edge version 92, you can turn off the warning "Disable developer mode extensions" by clicking on the 'Don't show this again' option. Please note: this is a Controlled Feature Rollout. If you don't see this feature, check back shortly as we continue our rollout.
- **Manage your extensions right from the toolbar**. The all-new extensions menu on the toolbar will allow you to hide/pin extensions easily. The quick links to manage extensions and find new extensions will make it easy for you to find new extensions and manage your existing ones. Please note: this is a Controlled Feature Rollout. If you don't see this feature, check back shortly as we continue our rollout.
- **Automatic HTTPS**. Users will have the option to upgrade navigation from HTTP to HTTPS on domains likely to support this more secure protocol. This support can also be configured to attempt delivery over HTTPS for all domains. Please note: we are experimenting with this feature and this behavior won't be seen if you have opted out of experiments.
- **Improvements to font rendering**. Improvements have been made to the rendering of text to improve clarity and reduce blurriness. Please note: this is a Controlled Feature Rollout. If you don't see this feature, check back shortly as we continue our rollout.

Policy updates

New policies

Eight new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added:

- AADWebSiteSSOUsingThisProfileEnabled Single sign-on for work or school sites using this profile enabled.
- AutomaticHttpsDefault Configure Automatic HTTPS
- HeadlessModeEnabled Control use of the Headless Mode
- InsecurePrivateNetworkRequestsAllowedSpecifies whether to allow insecure websites to make requests to more-private network endpoints
- InsecurePrivateNetworkRequestsAllowedForUrls Allow the listed sites to make requests to more-private network endpoints from insecure contexts
- InternetExplorerIntegrationLocalSiteListExpirationDays Specify the number of days that a site remains on the local IE mode site list
- InternetExplorerIntegrationReloadInIEModeAllowed Allow unconfigured sites to be reloaded in Internet Explorer mode
- SharedArrayBufferUnrestrictedAccessAllowed Specifies whether SharedArrayBuffers can be used in a non cross-origin-isolated context

Obsoleted Policy

- EnableSha1ForLocalAnchors Allow certificates signed using SHA-1 when issued by local trust anchors.

Version 92.0.902.9: June 8

Fixed various bugs and performance issues.

Version 91.0.864.41: June 3

Fixed various bugs and performance issues.

Version 91.0.864.37: May 27

Fixed various bugs and performance issues.

Version 91.0.864.36: May 26

Fixed various bugs and performance issues.

Version 91.0.864.33: May 21

Fixed various bugs and performance issues.

Version 91.0.864.27: May 14

Fixed various bugs and performance issues.

Version 91.0.864.19: May 7

Fixed various bugs and performance issues.

Version 91.0.864.15: May 3

Fixed various bugs and performance issues.

Version 91.0.864.11: April 30

Feature updates

- **Identify network traffic originating from Microsoft Defender Application Guard containers at the proxy level**. Starting with Microsoft Edge version 91, there's built in support to tag network traffic originating from Application Guard containers, allowing enterprises to identify them and apply specific policies.
- **Support option to allow synchronizing Favorites from the host to the Edge Application Guard container**. Starting with Microsoft Edge version 91, users have the option to configure Application Guard to synchronize their favorites from the host to the container. This ensures new favorites appear on the container as well.
- **Support for Speech Recognition APIs**. Starting with Microsoft Edge version 91, API support for speech recognition commands on Google.com and similar sites will be added. This feature is limited to a randomly selected group of users who have enabled experimentation. These users are giving feedback to the feature team.
- **Personalize your browser with new theme colors**. Make Microsoft Edge your own with one of the fourteen new theme colors on the Settings -> Appearance page. You can also install custom themes from the Microsoft Edge Add-on site. Learn more
- **Interrupt Downloads** Starting with Microsoft Edge version 91 the browser will automatically interrupt downloads of types which could harm your computer if those downloads are started without a user interaction and are not supported by SmartScreen Application Reputation check. Users may override and continue to download by right clicking and choosing "Keep" on the download item.

For more information, see Microsoft Edge Security downloads interruptions

Policy updates

New policies

Six new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added:

- ApplicationGuardTrafficIdentificationEnabled - Application Guard Traffic Identification
- ExplicitlyAllowedNetworkPorts - Explicitly allowed network ports
- ImportStartupPageSettings - Allow importing of startup page settings
- MathSolverEnabled - Let users snip a Math problem and get the solution with a step-by-step explanation in Microsoft Edge
- NewTabPageContentEnabled - Allow Microsoft News content on the new tab page
- NewTabPageQuickLinksEnabled - Allow quick links on the new tab page

Obsoleted Policy

- ProactiveAuthEnabled - Enable Proactive Authentication

Version 90.0.818.46: April 22

Fixed various bugs and performance issues.

Version 90.0.818.42: April 20

Fixed various bugs and performance issues.

Version 90.0.818.41: April 16

Fixed various bugs and performance issues.

Version 90.0.818.38: April 14

Fixed various bugs and performance issues.

Version 90.0.818.36: April 12

Fixed various bugs and performance issues.

Version 90.0.818.27: April 2

Fixed various bugs and performance issues.

Version 90.0.818.22: March 29

Fixed various bugs and performance issues.

Version 90.0.818.14: March 22

Fixed various bugs and performance issues.

Version 90.0.818.8: March 16

Feature updates

- Single Sign On (SSO) is now available for Azure Active Directory (Azure AD) accounts and

Microsoft Account (MSA) on macOS. A user signed in on Microsoft Edge on macOS will now get automatically signed into websites that are configured to allow single sign on with Work and Microsoft accounts (for example, bing.com, office.com, msn.com, and outlook.com).

- **Kiosk mode.** Starting with Microsoft Edge version 90, we have locked down the UI print settings to only allow the configured printers and "Print to PDF" options. We have also done improvements within the assigned access single app kiosk mode to restrict the launch of other applications from the browser. For more information about the kiosk mode features please go here.

- **Printing:**

  - **New print rasterization mode for non-PostScript printers**. Starting with Microsoft Edge version 90, Admins can use a new policy to define print rasterization mode for their users. This policy controls how Microsoft Edge prints to non-PostScript printers on Windows. Sometimes print jobs on non-PostScript printers need to be rasterized to print correctly. The print options are Full and Fast.

  - **Additional page scaling options for printing**. Users are now able to customize scaling while printing webpages and PDF documents using additional options. The "Fit to Page" option ensures that the webpage or document is fit into the space available in the selected "Paper size" for printing. The "Actual size" option ensures that there are no changes in the size of the contents being printed regardless of the selected "Paper size".

- **Productivity:**

  - **Autofill suggestions are extended to include address fields content from clipboard**. Clipboard content is parsed when you click on a profile/address field (for example, phone, email, zip code, city, state, etc.) to show as autofill suggestions.

  - **Users can search for autofill suggestions even if a form or field isn't detected**. Today if you have your information saved on Microsoft Edge, autofill suggestions pop up automatically and help you save time while filling out forms. In cases where autofill misses a form, or if you want to fetch data in forms that don't typically have autofill (like temporary forms), you can search for your information using autofill.

- **Access downloads from a flyout in the menu bar**. Downloads will appear in the top-right corner with all the active downloads in one place. This menu is easily dismissible so users can continue browsing uninterrupted, and they can monitor overall download progress right from the toolbar. Learn more.

Policy updates

New policies

Seven new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added:

- ApplicationGuardFavoritesSyncEnabled - Application Guard Favorites Sync Enabled
- ManagedConfigurationPerOrigin - Sets managed configuration values for websites to specific origins
- PrintRasterizationMode - Print Rasterization Mode
- QuickViewOfficeFilesEnabled - Manage QuickView Office files capability in Microsoft Edge
- SSLErrorOverrideAllowedForOrigins - Allow users to proceed from the HTTPS warning page for specific origins
- WindowOcclusionEnabled - Enable Window Occlusion
- WindowsHelloForHTTPAuthEnabled - Windows Hello For HTTP Auth Enabled

Deprecated policies

- NativeWindowOcclusionEnabled - Enable Native Window Occlusion
- SSLVersionMin- Minimum TLS version enabled

Version 89.0.774.54: March 13

Fixed various bugs and performance issues.

Version 89.0.774.50: March 10

Fixed various bugs and performance issues.

Version 89.0.774.48: March 8

Fixed various bugs and performance issues.

Version 89.0.774.45: March 3

Fixed various bugs and performance issues.

Version 89.0.774.39: February 26

Fixed various bugs and performance issues.

Version 89.0.774.34: February 22

Fixed various bugs and performance issues.

Version 89.0.774.27: February 12

Fixed various bugs and performance issues.

Version 89.0.774.23: February 8

Fixed various bugs and performance issues.

Version 89.0.774.18: February 3

Feature updates

- **Kiosk mode enables additional lockdown capabilities**. Starting with Microsoft Edge version 89, we have added additional lockdown capabilities within kiosk mode to enable customers to get the job done in a productive and more secure experience. Learn more.
- **The Enterprise Mode Site List Manager tool will be available in the browser through the *edge://compat* page**. You can use this tool to create, edit and export your site list XML for Internet Explorer mode on Microsoft Edge. You can enable access to this tool as needed through group policy. Learn More.
- **Improve browser performance with sleeping tabs**. Sleeping tabs improves browser performance by putting inactive tabs to sleep to free up system resources like memory and CPU so active tabs or other applications can use them. Users can prevent sites from going to sleep and configure the length of time before an inactive tab goes to sleep. To keep users in their flow, there are also heuristics to prevent certain sites from going to sleep, such as intranet sites. This feature can be managed with group policies.

  > **NOTE**
  > "Improve browser performance with sleeping tabs" is an update to the February 3 release notes for major version 89.0.774.18.

- **Reset your Microsoft Edge sync data in the cloud manually**. We are introducing a way to reset your Microsoft Edge sync data from within the product. This ensures that your data is cleared from Microsoft services, as well as resolving certain product issues that previously required a support ticket.
- **Improvements to text selection experience within PDF documents**. Users will begin to get a smoother and more consistent text selection experience across PDF documents opened in Microsoft Edge starting with version 89.
- **Date of birth field now supported in autofill**. Today Microsoft Edge helps you save time and effort while filling out forms and creating accounts online by auto filling your data like addresses, names, phone numbers, etc. Starting with Microsoft Edge version 89, we are adding support for another field that you can have saved and auto-filled - date of birth. You can view, edit and delete this information anytime in your profile settings.
- **Support for natural language search on the address bar, history search page, and the history hub**. Starting with Microsoft Edge version 89, finding an article/website will be easier with the natural language search on the address bar, history page, and history hub. Users can search for previously viewed page content/description/timing (such as "cake recipe from last week") in addition to titles/URL keyword matches. This feature is limited to a randomly selected group of users who have enabled experimentation. These users are giving feedback to the feature team.

Policy updates

New policies

- BrowsingDataLifetime - Browsing Data Lifetime Settings
- MAMEnabled - Mobile App Management Enabled
- DefinePreferredLanguages - Define an ordered list of preferred languages that websites should display in if the site supports the language
- ShowRecommendationsEnabled - Allow recommendations and promotional notifications from Microsoft Edge
- PrintingAllowedBackgroundGraphicsModes - Restrict background graphics printing mode
- PrintingBackgroundGraphicsDefault- Default background graphics printing mode
- SmartActionsBlockList- Block smart actions for a list of services

Obsoleted policies

- ForceLegacyDefaultReferrerPolicy - Use a default referrer policy of no-referrer-when-downgrade
- MetricsReportingEnabled - Enable usage and crash-related data reporting
- SendSiteInfoToImproveServices|Send site information to improve Microsoft services

Version 88.0.705.56: January 29

Fixed various bugs and performance issues.

Version 88.0.705.49: January 20

Fixed various bugs and performance issues.

Version 88.0.705.45: January 15

Fixed various bugs and performance issues.

Version 88.0.705.41: January 11

Fixed various bugs and performance issues.

Version 88.0.705.29: December 21

Fixed various bugs and performance issues.

Version 88.0.705.18: December 9

Feature updates

- **Deprecations:**
  - Deprecate support for FTP protocol. Support for the legacy FTP protocol has been removed from Microsoft Edge. Attempting to navigate to an FTP link will result in the browser directing the Operating System to open an external application to handle the FTP link. Alternatively, IT administrators can configure Microsoft Edge to use IE Mode for sites that rely on the FTP protocol.
  - Adobe Flash support will be removed. Starting with Microsoft Edge Beta version 88, Adobe Flash capability and support will be removed. Learn more: Update on Adobe Flash Player End of Support - Microsoft Edge Blog (windows.com)
- **Authentication:**
  - Single Sign On (SSO) now available for Azure Active Directory (Azure AD) accounts and Microsoft Account (MSA) on macOS and down-level Windows. A user signed in on Microsoft Edge on either macOS or down-level Microsoft Windows (7, 8.1) will now get automatically signed into websites that are configured to allow single sign on with Work and Microsoft accounts (e.g., bing.com, office.com, msn.com, outlook.com).
    Note: A user may have to sign out and then sign back in if they'd signed into Microsoft Edge in a version prior to Microsoft Edge 88 to leverage this feature.
  - Automatically switch users on macOS to their work profile for sites that authenticate with their work account. Starting with Microsoft Edge version 88, we provide the ability to switch sites that authenticate with a user's work profile on macOS.
    Note: A user may have to sign out and then sign back in if they'd signed into Microsoft Edge in a version prior to Microsoft Edge 88 to leverage this feature.
- **Kiosk mode option to end session**. The "End session" button is now available in a kiosk mode public browsing experience. This feature ensures that browser data and settings are deleted when Microsoft Edge is closed. Learn more about kiosk mode features and roadmap, Configure Microsoft Edge kiosk mode.
- **Security and Privacy:**
  - Alerts are generated if a user's password is found in an online leak. User passwords are checked against a repository of known-breached credentials and sends the user an alert if a match is found. To ensure security and privacy, user passwords are hashed and encrypted when they're checked against the database of leaked credentials.
  - Automatically upgrade mixed content. Secure pages delivered over HTTPS may contain references images that are served over non-secure HTTP. To improve privacy and security in Microsoft Edge 88, those images will be retrieved over HTTPS instead. If the image is not available over HTTPS, it will not be loaded.
  - View site permissions by site and by recent activity. Starting with Microsoft Edge 88, users will be able to manage site permissions more easily. They will be able to view permissions by web site rather than just permission type. Additionally, we've added a recent activity section that will show a user all the recent changes to their site permissions.
  - Increased controls for browser cookies. Starting with Microsoft Edge 88, users can delete third party cookies without affecting first party cookies. Users will also be able to filter their cookies by first or third party and sort by name, number of cookies, and the amount of data stored and last modified.
- **Performance:**

- Improve browser performance with sleeping tabs. Sleeping tabs improves browser performance by putting inactive tabs to sleep to free up system resources like memory and CPU so active tabs or other applications can use them. Users can prevent sites from going to sleep and configure the length of time before an inactive tab goes to sleep. To keep users in their flow, there are also heuristics to prevent certain sites from going to sleep, such as intranet sites. This feature is limited to a randomly selected group of users who have enabled experimentation. We are planning to have the sleeping tabs feature enabled by default with Microsoft Edge version 89. This feature can be managed with group policies.
- Improve Microsoft Edge startup speed with startup boost. To improve Microsoft Edge startup speed, we've developed a feature named startup boost. Startup boost makes Microsoft Edge launch faster by enabling Microsoft Edge to run in the background. Note: This feature is limited to a randomly selected group of users who have enabled experimentation. These users are giving feedback to the feature team.

- **Productivity:**
  - Improve productivity and multi-tasking with vertical tabs. As the number of horizontal tabs grows, site titles start to get cut off and tab controls are lost as each tab shrinks. This interrupts user workflow as they spend more time finding, switching, and managing their tabs and less time on the task at hand. Vertical tabs let users move their tabs to the side, where vertically aligned icons and longer site titles make it easier to quickly scan, identify and switch to the tab they want to open.
  - Auto filling the date of birth field. Microsoft Edge already helps save time and effort while filling out forms and creating accounts online by auto filling user data such as addresses, names, phone numbers, etc. Microsoft Edge now supports the date of birth field which users can save and auto fill. A user can view, edit and delete this information anytime in their profile settings.
  - Improvements to Recently closed in History. Recently closed now keeps the last 25 tabs and windows from any past browsing session rather than just the previous session. Users can select Recently closed in the new History experience to see all the tabs that were open.
  - "Your day at a glance" feature enabled by default. Starting with Microsoft Edge version 88, information workers can benefit from intelligent productivity features on their New tab page (NTP). We offer users signed in with their work or school account personalized and relevant content powered by their M365 Graph. Users can quickly scan their "Your day at a glance" modules to easily track their meetings and recent work as well as quickly launch the applications they want to use.
- **PDF:**
  - PDF document display in book view (two page). Starting with Microsoft Edge version 88, users can view PDF documents in a single page or in the two page book view. To change the view, click the **Page View** button in the toolbar.
  - Anchored text notes support for PDF files. Starting with Microsoft Edge version 87, users can add typed text notes on any piece of text in PDF files.
  - Smoother text selection experience in PDF documents. Users will get a smoother and consistent text selection experience across PDF documents opened in Microsoft Edge.
  - View webpages saved as PDF files in the Downloads bar. Users can now view the PDF files generated by setting "Save as PDF" as the printer destination for webpages in the Downloads bar.
- **Fonts:**
  - Browser icons are updated to the Fluent design system. As part of our continued work around Fluent Design in the browser, we've made changes to closer align icons to the new Microsoft icon system. These changes will impact many of our high-touch user interfaces, including tabs, address bar, as well as navigational and wayfinding icons found in our various menus.
  - Improved font rendering. Text rendering is improved for better clarity and to reduce blurriness.

Policy updates

New policies

Sixteen new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added.

- BlockExternalExtensions - Blocks external extensions from being installed.
- InternetExplorerIntegrationLocalFileAllowed - Allow launching of local files in Internet Explorer mode.
- InternetExplorerIntegrationLocalFileExtensionAllowList - Open local files in Internet Explorer mode file extension allow list.
- InternetExplorerIntegrationLocalFileShowContextMenu - Show context menu to open a link in Internet Explorer mode.
- IntranetRedirectBehavior - Intranet Redirection Behavior.
- PrinterTypeDenyList - Disable printer types on the deny list.
- ShowMicrosoftRewards - Show Microsoft Rewards experiences.
- SleepingTabsEnabled - Configure Sleeping Tabs.
- SleepingTabsTimeout - Set the background tab inactivity timeout for Sleeping Tabs.
- SleepingTabsBlockedForUrls - Block Sleeping Tabs on specific sites.
- StartupBoostEnabled - Enable startup boost.
- UpdatePolicyOverride - Specifies how Microsoft Edge Update handles available updates from Microsoft Edge.
- VerticalTabsAllowed - Configures availability of a vertical layout for tabs on the side of the browser.
- WebRtcAllowLegacyTLSProtocols - Allow legacy TLS/DTLS downgrade in WebRTC.

Deprecated policies

The following policies are deprecated.

- ProactiveAuthEnabled - Enable Proactive Authentication.
- ProxyBypassList - Configure proxy bypass rules.
- ProxyMode - Configure proxy server settings.
- ProxyPacUrl - Set the proxy .pac file URL.
- ProxyServer - Configure address or URL of proxy server.
- WebDriverOverridesIncompatiblePolicies - Allow WebDriver to Override Incompatible Policies.

Obsoleted policies

The following policies are obsoleted.

- DefaultPluginsSetting - Default Adobe Flash setting.
- PluginsAllowedForUrls - Allow the Adobe Flash plug-in on specific sites.
- PluginsBlockedForUrls - Block the Adobe Flash plug-in on specific sites.
- RunAllFlashInAllowMode - Extend Adobe Flash content setting to all content.

Version 87.0.664.55: December 3

Fixed various bugs and performance issues. The following new feature is supported in this release.

- **Alerts are generated if a user's password is found in an online leak**. User passwords are checked against a repository of known-breached credentials and sends the user an alert if a match is found. To ensure security and privacy, user passwords are hashed and encrypted when they're checked against the database of leaked credentials.

Version 87.0.664.52: November 30

Fixed various bugs and performance issues.

Version 87.0.664.40: November 18

Fixed various bugs and performance issues.

Version 87.0.664.36: November 16

Fixed various bugs and performance issues.

Version 87.0.664.30: November 9

Fixed various bugs and performance issues.

Version 87.0.664.24: November 2

Fixed various bugs and performance issues.

Version 87.0.664.18: October 26

Fixed various bugs and performance issues.

Version 87.0.664.12: October 20

Feature updates

- **Kiosk mode privacy features enabled**. Starting with Microsoft Edge version 87 kiosk mode features that will help enterprises around the privacy of user data will be enabled. These features will enable experiences such as clear the user data on exit, delete downloaded files and to reset the configured start experience after a specified amount of idle time. Learn more about how to Configure Microsoft Edge kiosk mode
- **ClickOnce deployment enabled by default**. ClickOnce is enabled by default in Microsoft Edge 87, which reduces the barriers for enterprises to deploy software and better align with Microsoft Edge Legacy browser behavior. Starting in Microsoft Edge 87, the ClickOnceEnabled policy's "Not configured" state will reflect the new default ClickOnce state of Enabled (as compared to the previous default state of Disabled).
- **The enterprise new tab page (NTP) integrates productivity with customizable, work-relevant feed content**. The enterprise NTP blends the Office 365 productivity page we offer to users signed in with their work or school account with personalized, work-relevant company and industry feeds that are organized in a single page. Users will be able to recognize the familiar Office 365 content and Microsoft Search for Business powered by Bing. In addition, they can easily flip to a customizable "My Feed" with content and modules that are relevant to the user, their company, or their industry, as well as a selection of other feeds that the organization has made available. Learn more.
- **Privacy and Security:**
    - Support TLS Token Binding for policy-configured sites. TLS Token binding helps prevent token theft attacks to ensure that cookies can't be reused from a device other than the device upon which they were initially set. The use of TLS token binding requires setting the AllowTokenBindingForUrls policy and requires that the sites listed support this feature.
- **Keyboard support for highlighter on PDF files**. Users can use their keyboard keys to highlight any text on a PDF.
- **Printing:**
    - Choose which side to flip on when printing on both sides. Users can choose to flip on the long side or the short side of a sheet when printing on both sides.

- Choose print rasterization mode for the enterprise. Control how Microsoft Edge prints to a non-PostScript printer on Windows. Sometimes print jobs on non-PostScript printers need to be rasterized to print correctly. The print options are "Full" and "Fast".

Policy updates

New policies

Ten new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added.

- ConfigureFriendlyURLFormat - Configure the default paste format of URLs copied from Microsoft Edge, and determine if additional formats will be available to users.
- EdgeShoppingAssistantEnabled - Shopping in Microsoft Edge Enabled.
- HideInternetExplorerRedirectUXForIncompatibleSitesEnabled - Hide the one-time redirection dialog and the banner on Microsoft Edge.
- KioskAddressBarEditingEnabled - Configure address bar editing for kiosk mode public browsing experience.
- KioskDeleteDownloadsOnExit - Delete files downloaded as part of kiosk session when Microsoft Edge closes.
- PasswordRevealEnabled - Enable the Password reveal button.
- RedirectSitesFromInternetExplorerPreventBHOInstall - Prevent install of the BHO to redirect incompatible sites from Internet Explorer to Microsoft Edge.
- RedirectSitesFromInternetExplorerRedirectMode - Redirect incompatible sites from Internet Explorer to Microsoft Edge.
- SpeechRecognitionEnabled - Configure Speech Recognition.
- WebCaptureEnabled - Enable the web capture feature in Microsoft Edge.

Deprecated Policy

NewTabPageSetFeedType - Configure the Microsoft Edge new tab page experience.

Obsoleted Policy

EnableDeprecatedWebPlatformFeatures - Re-enable deprecated web platform features for a limited time.

Version 86.0.622.43: October 16

Fixed various bugs and performance issues.

Version 86.0.622.36: October 7

Fixed various bugs and performance issues.

Version 86.0.622.31: October 1

Fixed various bugs and performance issues.

Version 86.0.622.28: September 28

Fixed various bugs and performance issues.

Version 86.0.622.15: September 14

Fixed various bugs and performance issues.

Version 86.0.622.11: September 9

Feature updates

- Internet Explorer mode:

  - Let users use the Microsoft Edge User Interface (UI) to test sites in Internet Explorer mode. Beginning with Microsoft Edge version 86, administrators can enable a UI option for their users to load a tab in Internet Explorer mode for testing purposes or as a stopgap until sites are added to the site list XML.
- **Delete downloads from disk using download manager.** Users are now able to delete their downloaded files from their disk without leaving the browser. The new Delete downloads functionality exists within the context menu of downloads shelf or the downloads page.
- **Roll back to previous Microsoft Edge version.** The rollback feature lets administrators revert to a known good version of Microsoft Edge if there's an issue in the latest version of Microsoft Edge. Learn more.
- **Enforce enabling Sync by default across the enterprise.** Administrators can enable synchronization for Azure Active Directory (Azure AD) accounts by default with the ForceSync policy.
- **PDF updates:**
  - Table of contents for PDF Documents. Beginning with version 86, Microsoft Edge has added support for table of contents that lets users easily navigate through PDF documents.
  - Access all PDF functionalities on small form factor screens. Access all the capabilities of the Microsoft Edge PDF reader on devices with small screen sizes.
  - Pen support for highlighter on PDF files. With this update, users can use their digital pen to directly highlight text on PDF files, in the same way they would with a physical highlighter and paper.
  - Improved PDF scrolling. You will now be able to experience stutter free scrolling while navigating through long PDF documents.
- **Automatic profile switching on Windows 7, 8, and 8.1.** The automatic profile switching currently available in Microsoft Edge on Windows 10 is extended to downlevel Windows (Windows 7, 8,and 8.1). For more information, see the automatic profile switching blog post.
- **Users will see auto complete suggestions when they start typing a search query on the Microsoft Edge Add-ons website.** Auto complete will help users quickly complete their search query without having to type the entire string. This will be helpful because users won't have to remember correct spellings and they can choose from the available options that are displayed.
- **Remove the HTML5 Application Cache API.** Beginning with Microsoft Edge version 86, the legacy Application Cache API that enables offline use of web pages is being removed from Microsoft Edge. Web Developers should review the WebDev documentation for information on replacing the Application Cache API with Service Workers. Important: You can request an AppCache OriginTrial Token that allows sites to continue to use the deprecated Application Cache API until Microsoft Edge version 90.
- **Security:**
  - Secure DNS (DNS-over-HTTPS) Support. Beginning with Microsoft Edge version 86, settings to control Secure DNS on un-managed devices is available. These settings aren't accessible to users on managed devices, but IT admins can enable or disable Secure DNS using the dnsoverhttpsmode group policy.
- **Add a custom image to the New Tab Page (NTP) using a group policy.** Beginning with Microsoft Edge version 86 the NTP has an option to replace the default image with a custom user-supplied image. The ability to manage the properties of this image is also supported by the group policy.
- **Match customized keyboard shortcuts to VS Code.** Microsoft Edge DevTools now supports customizing keyboard shortcuts in the DevTools to match with your editor/IDE. (In Microsoft Edge 84, we added the ability to match DevTools keyboard shortcuts to VS Code).
- **Replace MetricsReportingEnabled and SendSiteInformationToImproveServices policies for downlevel Windows and macOS.** These policies are deprecated in Microsoft Edge version 86 and will become obsolete in Microsoft Edge version 89.

These policies are replaced by Allow Telemetry on Windows 10, and the new DiagnosticData policy for all other platforms. This will let users manage the diagnostic data that gets sent to Microsoft for Windows 7, 8, 8.1 and macOS.

- **SameSite=Lax Cookies By Default**. To improve web security and privacy, cookies will now default to SameSite=Lax handling by default. This means that cookies will only be sent in a first-party context and will be omitted for requests sent to third-parties. This change can cause compatibility impact on websites that require cookies for third-party resources to function correctly. To permit such cookies, web developers can mark cookies which should be set from and sent to third-party contexts by adding explicit `SameSite=none` and `Secure` attributes when the cookie is set. Enterprises that wish to exempt certain sites from this change can do so using the LegacySameSiteCookieBehaviorEnabledForDomainList policy, or can opt-out of the change across all sites using the LegacySameSiteCookieBehaviorEnabled policy.

Policy updates

New policies

Nineteen new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added.

- CollectionsServicesAndExportsBlockList - Block access to a specified list of services and export targets in Collections.
- DefaultSensorsSetting - Default sensors setting.
- DefaultSerialGuardSetting - Control use of the Serial API.
- DiagnosticData - Send required and optional diagnostic data about browser usage.
- EnterpriseModeSiteListManagerAllowed - Allow access to the Enterprise Mode Site List Manager tool.
- ForceSync - Force synchronization of browser data and do not show the sync consent prompt.
- InsecureFormsWarningsEnabled - Enable warnings for insecure forms.
- InternetExplorerIntegrationTestingAllowed - Allow Internet Explorer mode testing.
- SpotlightExperiencesAndRecommendationsEnabled - Choose whether users can receive customized background images and text, suggestions, notifications, and tips for Microsoft services.
- NewTabPageAllowedBackgroundTypes - Configure the background types allowed for the new tab page layout.
- SaveCookiesOnExit - Save cookies when Microsoft Edge closes.
- SensorsAllowedForUrls - Allow access to sensors on specific sites.
- SensorsBlockedForUrls - Block access to sensors on specific sites.
- SerialAskForUrls - Allow the Serial API on specific sites.
- SerialBlockedForUrls - Block the Serial API on specific sites.
- URLBlocklist - Block access to a list of URLs.
- URLAllowlist - Define a list of allowed URLs.
- UserAgentClientHintsEnabled - Enable the User-Agent Client Hints feature.
- UserDataSnapshotRetentionLimit - Limits the number of user data snapshots retained for use in case of emergency rollback.

Deprecated Policies

- MetricsReportingEnabled - Enable usage and crash-related data reporting.
- SendSiteInfoToImproveServices - Send site information to improve Microsoft services.

Obsoleted Policy

TLS13HardeningForLocalAnchorsEnabled - Enable a TLS 1.3 security feature for local trust anchors.

Policy caption changed

NativeWindowOcclusionEnabled - Enable Native Window Occlusion.

Policy description changed

- AdsSettingForIntrusiveAdsSites
- AllowTokenBindingForUrls
- AmbientAuthenticationInPrivateModesEnabled
- ApplicationGuardContainerProxy
- AutoImportAtFirstRun
- AutoOpenFileTypes
- BrowserSignin
- ClearBrowsingDataOnExit
- ClickOnceEnabled
- CommandLineFlagSecurityWarningsEnabled
- ConfigureOnPremisesAccountAutoSignIn
- ConfigureShare
- CookiesAllowedForUrls
- CustomHelpLink
- DefaultCookiesSetting
- DefaultGeolocationSetting
- DefaultImagesSetting
- DefaultInsecureContentSetting
- DefaultJavaScriptSetting
- DefaultNotificationsSetting
- DefaultPluginsSetting
- DefaultPopupsSetting
- DefaultSearchProviderEnabled
- DefaultWebBluetoothGuardSetting
- DefaultWebUsbGuardSetting
- DelayNavigationsForInitialSiteListDownload
- DeveloperToolsAvailability
- EnableSha1ForLocalAnchors
- DownloadRestrictions
- EnableDeprecatedWebPlatformFeatures
- WinHttpProxyResolverEnabled
- ExperimentationAndConfigurationServiceControl
- ExternalProtocolDialogShowAlwaysOpenCheckbox
- ExtensionInstallForcelist
- ForceBingSafeSearch
- ForceYouTubeRestrict
- HomepageIsNewTabPage
- HomepageLocation
- InPrivateModeAvailability
- InternetExplorerIntegrationEnhancedHangDetection
- InternetExplorerIntegrationLevel
- InternetExplorerIntegrationSiteRedirect
- LegacySameSiteCookieBehaviorEnabled
- NativeWindowOcclusionEnabled
- NavigationDelayForInitialSiteListDownloadTimeout
- NetworkPredictionOptions

- NewTabPageLocation
- NewTabPageSearchBox
- NewTabPageSetFeedType
- NonRemovableProfileEnabled
- PasswordProtectionWarningTrigger
- PasswordProtectionLoginURLs
- PasswordProtectionChangePasswordURL
- PluginsAllowedForUrls
- PluginsBlockedForUrls
- PreventSmartScreenPromptOverride
- PreventSmartScreenPromptOverrideForFiles
- ProxyMode
- RegisteredProtocolHandlers
- RelaunchNotification
- RestoreOnStartup
- RestoreOnStartupURLs
- RestrictSigninToPattern
- SSLVersionMin
- SmartScreenAllowListDomains
- SmartScreenEnabled
- SmartScreenForTrustedDownloadsEnabled
- SmartScreenPuaEnabled
- SyncTypesListDisabled
- TrackingPrevention
- WebRtcLocalhostIpHandling

Version 85.0.564.41: August 25

Fixed various bugs and performance issues.

Version 85.0.564.40: August 21

Fixed various bugs and performance issues.

Version 85.0.564.36: August 17

Fixed various bugs and performance issues.

Version 85.0.564.30: August 10

Fixed various bugs and performance issues.

Version 85.0.564.23: August 3

Fixed various bugs and performance issues.

Version 85.0.564.18: July 28

Feature updates

- **On-premises synchronization of Favorites and Settings**. Now you can synchronize browser

favorites and settings between Active Directory profiles within your own environment without the need for cloud sync.

- **Microsoft Edge group policy support for trusting site + app combos to launch without a confirmation prompt.** Group policy support added that lets administrators add site + app combos that are trusted to launch without the confirmation prompt. This adds the ability for administrators to configure trusted protocol/origin combinations (such as Microsoft 365 apps) for their end-users to suppress the confirmation prompt when navigating to a URL that contains an app protocol.
- **PDF Highlighter tool**. This tool can be added to the toolbar for PDFs to easily highlight important text.
- **The Storage Access API is available**. The Storage Access API allows access to first-party storage in a third-party context when a user has provided a direct intent to allow storage that would otherwise be blocked by the browser's current configuration. For more information, see Storage Access API.
- **Send to OneNote is available for Microsoft Edge Collections**. Everyone's excited to be able to send the information they've gathered in Collections to OneNote, where they can append it to a larger project and collaborate with others! And even more importantly, in Microsoft Edge 85, you'll be able send content to *Office for Mac* products (Word, Excel, and OneNote) for both Microsoft account and Azure Active Directory.
- **DevTools updates**. For details about the following updates, see What's New In DevTools (Microsoft Edge 85).
    - Microsoft Edge DevTools supports Surface Duo emulation. The Microsoft Edge DevTools can emulate the Surface Duo so you can test how your web content will look on dual-screen devices. To turn on this experiment in DevTools, enter Device Mode by pressing Ctrl+Shift+M on Windows or Command+Shift+M on macOS, and then select Surface Duo from the device drop-down list.
    - Microsoft Edge DevTools lets you match keyboard shortcuts to VS Code. The Microsoft Edge DevTools supports customizing keyboard shortcuts in the DevTools to match your editor/IDE. In Microsoft Edge 85, we are adding the ability to match DevTools keyboard shortcuts to VS Code. This change will help increase productively across VS Code and DevTools.

Policy updates

New policies

Thirteen new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added.

- AutoLaunchProtocolsFromOrigins - Define a list of protocols that can launch an external application from listed origins without prompting the user.
- AutoOpenAllowedForURLs - URLs where AutoOpenFileTypes can apply.
- AutoOpenFileTypes - List of file types that should be automatically opened on download.
- DefaultSearchProviderContextMenuAccessAllowed - Allow default search provider context menu search access.
- EnableSha1ForLocalAnchors - Allow certificates signed using SHA-1 when issued by local trust anchors.
- IntensiveWakeUpThrottlingEnabled - Control the IntensiveWakeUpThrottling feature.
- NewTabPagePrerenderEnabled - Enable preload of the new tab page for faster rendering.
- NewTabPageSearchBox - Configure the new tab page search box experience.
- PasswordMonitorAllowed - Allow users to be alerted if their passwords are found to be unsafe.
- RoamingProfileSupportEnabled - Enable using roaming copies for Microsoft Edge profile data.
- RoamingProfileLocation - Set the roaming profile directory.
- TLSCipherSuiteDenyList - Specify the TLS cipher suites to disable.

Obsoleted policies

- EnableDomainActionsDownload - Enable Domain Actions Download from Microsoft.
- WebComponentsV0Enabled - Re-enable Web Components v0 API until M84.
- WebDriverOverridesIncompatiblePolicies- Allow WebDriver to Override Incompatible Policies.

Version 84.0.522.35: July 9

Fixed various bugs and performance issues.

Version 84.0.522.28: June 26

Fixed various bugs and performance issues.

Version 84.0.522.26: June 24

Fixed various bugs and performance issues.

Version 84.0.522.20: June 15

Fixed various bugs and performance issues.

Version 84.0.522.15: June 8

Fixed various bugs and performance issues.

Version 84.0.522.11: June 2

Feature updates

- This version of Microsoft Edge provides improved site list download times for Internet Explorer mode. We've reduced download delay for the Internet Explorer mode site list to 0 seconds (down from a 60-second wait) in the absence of a cached site list. We've also added group policy support for cases when Internet Explorer mode home page navigations need to be delayed until the site list is downloaded. For more information, see the DelayNavigationsForInitialSiteListDownload policy.
- Microsoft Edge now allows users to sign-into the browser when it's "run as administrator" on Windows 10. This will help customers running Microsoft Edge on Windows server or in remote-desktop and sandbox scenarios.
- Microsoft Edge now provides full mouse support when in full screen mode. Now you can use your mouse to access tabs, the address bar, and other items without having to exit full screen mode.
- Online purchase improvement. Add custom nicknames to saved debit or credit cards. Now you can distinguish and differentiate your credit cards when making online purchases. Nicknaming your debit or credit cards lets you choose the correct card when using autofill to select a payment method.
- TLS/1.0 and TLS/1.1 are disabled by default. To help discover impacted sites, you can set the *edge://flags/#display-legacy-tls-warnings* flag to cause Microsoft Edge to display a non-blocking "Not Secure" notice when loading pages that require legacy TLS protocols. The SSLVersionMin policy permits re-enabling of TLS/1.0 and TLS/1.1. This policy will remain available until at least Microsoft Edge version 88. For more information, see Site compatibility-impacting changes coming to Microsoft Edge.
- Collections improvements:
    - A note capability is added that lets you add a note or comment to an item in a collection. Notes are grouped together and stay attached to an item even if you sort the items in a collection. To try this new feature, right-click on an item and select "Add note".

    - You can change the background color of notes in collections. You can use color coding to help you organize information and increase productivity.
    - There are noticeable performance improvements, which lets you export your collections to Excel in less time than in previous versions of Microsoft Edge.
- Additional Microsoft Edge API support:
    - The Storage Access API. This API allows access to first-party storage in a third-party context when a user provides a direct intent to allow storage that would otherwise be blocked by the browser's current configuration.

      As privacy is becoming increasingly important to users, requests for stricter browser defaults and user opt-in settings like blocking all third-party storage access are increasingly common. While these settings help improve privacy and block unwanted access by unknown or untrusted parties, they can have unwanted side effects such as blocking access to content the user may want to view (for example, social media and embedded media content.)
    - The Native File System API, which means you can give sites permissions to edit files or folders via the Native File System API.
- PDF improvements:
    - Read Aloud for PDF lets users listen to PDF content while carrying out other tasks that may be important for them. It also helps audio visual learners focus on reading the content, making learning easier.
    - PDF file editing is improved. Now you can save an edit made to a PDF back to the file instead of saving a copy each time you edit the PDF.
- Microsoft Edge now enables Translation in the Immersive Reader. When a user opens the Immersive Reader view, they get the option to translate the page to their desired language.
- DevTools supports customizing keyboard shortcuts to match your editor/IDE, which includes VS Code.

Policy updates

New policies

Five new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added.

- AppCacheForceEnabled - Allows the AppCache feature to be re-enabled, even if it's turned off by default.
- ApplicationGuardContainerProxy - Application Guard Container Proxy.
- DelayNavigationsForInitialSiteListDownload - Require that the Enterprise Mode Site List is available before tab navigation.
- NativeWindowOcclusionEnabled - Enable Hiding of Native Windows.
- NavigationDelayForInitialSiteListDownloadTimeout - Set a timeout for delay of tab navigation for the Enterprise Mode Site List.

Deprecated policies

- AllowSyncXHRInPageDismissal - Allow pages to send synchronous XHR requests during page dismissal.
- BuiltinCertificateVerifierEnabled - Determines whether the built-in certificate verifier will be used to verify server certificates.
- StricterMixedContentTreatmentEnabled - Enable stricter treatment for mixed content.

Obsoleted policy

ForceNetworkInProcess - Force networking code to run in the browser process.

Version 83.0.478.44: June 1

Fixed various bugs and performance issues.

Version 83.0.478.37: May 20

Fixed various bugs and performance issues.

Version 83.0.478.33: May 15

Fixed various bugs and performance issues.

Version 83.0.478.28: May 7

Fixed various bugs and performance issues.

Version 83.0.478.25: May 4

Fixed various bugs and performance issues.

Version 83.0.478.18: April 27

Fixed various bugs and performance issues.

Version 83.0.478.13: April 22

Feature updates

- Microsoft Defender SmartScreen improvements: Made several improvements to the Microsoft Defender SmartScreen service, such as improved protection from malicious sites that redirect when loading, and top-level frame blocking, which completely replaces malicious sites with the Microsoft Defender SmartScreen safety page. The top-level frame blocking prevents audio and other media from the malicious site from playing which gives an easier and less confusing experience.
- In response to user feedback, users can now exempt certain cookies from automatically clearing when the browser closes. This option is helpful if there's a site that users don't want to be signed out of, but still want to have all the other cookies cleared when the browser closes. To use this feature, go to *edge://settings/clearBrowsingDataOnClose* and enable the "Cookies and other site data" toggle.
- Automatic Profile Switching is now available to help you get to your work content more easily across profiles. If you use multiple profiles at work, you can check it out by navigating to a site requiring authentication from your work or school account while on your personal profile. When we detect a change, you will receive a prompt to switch to your work profile to access that site without having to authenticate to it. When you choose the work profile you want to switch to, the website will open in your work profile. This profile switching capability will help you keep your work and personal data separate and help you get to your work content more effortlessly. If you don't want the feature to prompt you to switch profiles, you can choose the don't ask me again option and it will get out of your way.
- Collections feature improvements:
    - You can use drag and drop to add an item to a collection without opening the collection. During the drag and drop you can also choose a location in the collection list where you want to put the item.
    - You can add multiple items to a collection instead of adding one item at a time. To add multiple items, select the items and then drag them to a collection. Or you can select the items, right-click and then pick the collection where you want the items.
- You can add all the tabs in an Edge window into a new collection without adding them individually. To add all the tabs, right-click on any tab and choose "Add all tabs to a new collection".

- Extension sync is now available. You can now sync your extensions across all your devices! Extensions from both the Microsoft and Chrome Stores will sync with Microsoft Edge. To use this feature: Click the ellipses (...) on the menu bar, select **Settings**. Under Your profile, click **Sync** to see the Sync options. Under **Profiles/Sync** use the toggle to enable Extensions. You can use the SyncTypesListDisabled group policy to disable syncing of extensions.
- Improved the message on the Downloads management page for insecure downloads that have been blocked.
- Immersive Reader improvements:
  - Added support for Adverbs in the Parts of Speech experience we have in Immersive Reader. While reading an article within the Immersive Reader, open the Grammar Tools and switch on Adverbs within Parts of Speech to highlight all the adverbs on the page.
  - Added the ability to select any content on a webpage and open it in Immersive Reader. This ability enables users to use the Immersive Reader and all the Learning Tools, such as Line Focus and Read Aloud, across all websites.
- Link doctor provides host correction and a search query to the users when they mistype a URL. For example:
  A user mistypes "powerbi as "powerbbi".com. Link doctor will suggest "powerbi".com as a correction and create a link to search for "powerbbi" in case the user is looking for something different.
- Allow users to save their decision to launch an external protocol for a specific site. Users can configure the ExternalProtocolDialogShowAlwaysOpenCheckbox policy to enable or disable this feature.
- Users can set Microsoft Edge as their default browser directly from Microsoft Edge **Settings**. This capability makes it easier for users to change their default browser, within the context of the browser itself, instead of having to search through the operating system settings. To use this feature, go to *edge://settings/defaultBrowser* and click **Make default**.
- Several DevTools updates, including new remote debugging support, UI improvements, and more. For more information, see What's New In DevTools (Microsoft Edge 83).

Policy updates

New policies

15 new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added.

- AllowSurfGame - Allow surf game.
- AllowTokenBindingForUrls - Configure the list of sites for which Microsoft Edge will attempt to establish a Token Binding with.
- BingAdsSuppression - Block all ads on Bing search results.
- BuiltinCertificateVerifierEnabled - Determines whether the built-in certificate verifier will be used to verify server certificates.
- ClearCachedImagesAndFilesOnExit - Clear cached images and files when Microsoft Edge closes.
- ConfigureShare - Configure the Share experience.
- DeleteDataOnMigration - Delete old browser data on migration.
- DnsOverHttpsMode - Control the mode of DNS-over-HTTPS.
- DnsOverHttpsTemplates - Specify URI template of desired DNS-over-HTTPS resolver.
- FamilySafetySettingsEnabled - Allow users to configure Family safety.
- LocalProvidersEnabled - Allow suggestions from local providers.
- ScrollToTextFragmentEnabled - Enable scrolling to text specified in URL fragments.
- ScreenCaptureAllowed - Allow or deny screen capture.

- SyncTypesListDisabled - Configure the list of types that are excluded from synchronization.
- NativeWindowOcclusionEnabled - Enable Hiding of Native Windows.

Deprecated policy

The following policy will continue to work in this release. It will become "obsolete" in a future release.

EnableDomainActionsDownload Enable Domain Actions Download from Microsoft

Version 81.0.416.60: April 20

Fixed various bugs and performance issues.

Version 81.0.416.58: April 17

Security updates.

Version 81.0.416.50: April 10

Fixed various bugs and performance issues.

Version 81.0.416.45: April 3

Fixed various bugs and performance issues.

Version 81.0.416.41: March 30

Fixed various bugs and performance issues.

Version 81.0.416.34: March 17

Fixed various bugs and performance issues.

Version 81.0.416.31: March 12

Fixed various bugs and performance issues.

Version 81.0.416.28: March 9

Fixed various bugs and performance issues.

Version 81.0.416.20: February 28

Fixed various bugs and performance issues.

Version 81.0.416.12: February 20

Feature updates

- Collections is now available. You can get started by clicking the Collections icon next to the address bar. This action opens the Collections pane where you can create, edit, and view Collections. We designed Collections based on what you do on the web. If you're a shopper, a traveler, a teacher, or a student, Collections can help. Learn more.
- Allow the removal (Hide from toolbar) of the Collections button from the Microsoft Edge toolbar for consistency.

- On-prem Active Directory account auto sign in will only be targeted to organizations that turn it on. If users were already signed in with an on-prem AD account, they will now be able to sign out of it. Now, users will only be automatically signed in with the primary account on their operating system if it is a Microsoft account or an Azure Active Directory account. Admins can enable auto sign in with an on-prem AD account using the ConfigureOnPremisesAccountAutoSignIn policy.
- Application Guard. Extensions support now available in the container.
- Added a message to inform users that Internet Explorer isn't installed when they navigate to a page that is configured to open in Internet Explorer mode.
- Updated the 3D View tool in Microsoft Edge DevTools with a new feature to help debug z-index stacking context. 3D View shows a representation of the DOM (Document Object Model) depth using color and stacking, and the z-Index view helps you isolate the different stacking contexts of your page. Learn more.
- Localized the F12 Dev tools in 10 new languages, so they will match the language used in the rest of the browser. Learn more.
- Added support for Dolby Vision playback. On Dolby Vision-enabled Windows 10 Build 17134 (April 2018 Update), websites can show Dolby vision content. See how to enable Dolby Vision content from Netflix.
- Microsoft Edge can now identify and remove duplicate favorites and merge folders with the same name. To access the tool, click the star on the browser's toolbar and select "Remove duplicate favorites". You will be able to confirm changes and any updates to your favorites will be synced across devices.
- We heard from users it can be difficult to distinguish a normal browsing window in dark theme from an InPrivate window since both window frames are dark. The new solid InPrivate blue pill in the top right corner helps reassure users they are browsing InPrivate.
- Open external links in the correct browser profile. Select a default profile for links opened for external apps to open in from *edge://settings/multiProfileSettings*.
- Added a warning to alert users who sign into a browser profile with an account after being previously signed in with another account. This will help prevent unintentional data merging.
- If you have payment cards saved in your Microsoft account, you can use them in Microsoft Edge while filling out payment forms. The cards in your Microsoft account will sync across desktop devices and the full details will be shared with the website after two-factor authentication (CVC code and your Microsoft identity.) For further convenience, you can choose to securely save a copy of the card on the device during authentication.
- Line Focus is designed for users who like to focus on a limited part of the content as they read. It lets users keep the focus on 1, 3 or 5 lines at a time and dims out the rest of the page to let users read without distraction. Users can scroll using touch or arrow keys and the focus shifts accordingly.
- Microsoft Edge is now integrated with Windows Speller on Windows platforms 8.1 and above. This integration provides greater language support, with access to more language dictionaries and the ability to use Windows custom dictionaries. There is no further action needed from the users when a language has been added in the OS language settings and a language spellcheck toggle is enabled in Microsoft Edge settings.
- When PDF documents are opened using Microsoft Edge, users will now be able to create highlights, change color, and delete highlights. This helps in referencing important parts of the document later, and for collaboration.
- When loading long PDF documents that have been optimized for web, the pages being viewed by the user will be loaded faster, parallelly, while the rest of the document is loading.
- Now it's easier to start the Immersive Reader for a website by just pressing the F9 key.

- Now it's easier to start Read Aloud by using a keyboard shortcut (Ctrl + Shift + U).

Policy updates

New policies

12 new policies were added. Download the updated Administrative Templates from the Microsoft Edge Enterprise landing page. The following new policies were added.

- AmbientAuthenticationInPrivateModesEnabled - Enable Ambient Authentication for InPrivate and Guest profiles.
- AudioSandboxEnabled - Allow the audio sandbox to run.
- ForceLegacyDefaultReferrerPolicy - Use a default referrer policy of no-referrer-when-downgrade.
- GloballyScopeHTTPAuthCacheEnabled - Enable globally scoped HTTP auth cache.
- ImportExtensions - Allow importing of extensions.
- ImportCookies - Allow importing of Cookies.
- ImportShortcuts - Allow importing of shortcuts.
- InternetExplorerIntegrationSiteRedirect - Specify how "in-page" navigations to unconfigured sites behave when started from Internet Explorer mode pages.
- OmniboxMSBProviderEnabled - Enable Microsoft Search for Business provider in omnibox.
- StricterMixedContentTreatmentEnabled - Enable stricter treatment for mixed content.
- TLS13HardeningForLocalAnchorsEnabled - Enable a TLS 1.3 security feature for local trust anchors.
- ConfigureOnPremisesAccountAutoSignIn - Configure automatic sign in with an Active Directory domain account when there is no Azure AD domain account.

Deprecated policies

The following policies continue to work in this release. They will become "obsolete" in a future release.

- WebComponentsV0Enabled - Re-enable Web Components v0 API until M84.
- WebDriverOverridesIncompatiblePolicies - Allow WebDriver to Override Incompatible.

See also

- Microsoft Edge Enterprise landing page

Microsoft Edge release schedule

11/1/2022 • 2 minutes to read • Edit Online

This article describes the release cadence and anticipated release schedule for Microsoft Edge.

Release cadence

Microsoft provides four options, called channels, to manage how often Microsoft Edge is updated with new features. For more information about our channels, their release cycle, and support levels, see the Channel overview.

Starting with Stable channel version 94, Microsoft Edge is moving to a 4-week major release cycle cadence. However, we recognize that enterprise customers who manage complex environments need more time to plan and test Microsoft Edge updates. To help our enterprise customers who need an extended timeline to manage updates, Microsoft Edge will offer an **Extended Stable option aligned to a longer, 8-week major release cycle**. This option will only be available for customers with managed environments. For more information, see How to opt-in to the Extended Stable release cycle option beginning with Microsoft Edge 94

Release schedule

The following table lists the planned and actual release dates for major releases in the Beta, Stable, and Extended Stable channels.

> **NOTE**
> Release dates are approximate and might vary based on build status.

Microsoft Edge releases

VERSION	RELEASE STATUS	BETA CHANNEL RELEASE WEEK	STABLE CHANNEL RELEASE WEEK	EXTENDED STABLE CHANNEL RELEASE WEEK
88	Released Version	09-Dec-2020 88.0.705.18	21-Jan-2021 88.0.705.50	
89	Released Version	03-Feb-2021 89.0.774.18	08-Mar-2021 89.0.774.48	
90	Released Version	16-Mar-2021 90.0.818.8	15-Apr-2021 90.0.818.39	
91	Released Version	30-Apr-2021 91.0.864.11	27-May-2021 91.0.864.37	
92	Released Version	08-Jun-2021 92.0.902.9	22-July-2021 92.0.902.55	
93	Released Version	03-Aug-2021 93.0.961.11	02-Sep-2021 93.0.961.38	

VERSION	RELEASE STATUS	BETA CHANNEL RELEASE WEEK	STABLE CHANNEL RELEASE WEEK	EXTENDED STABLE CHANNEL RELEASE WEEK
94	Released Version	02-Sep-2021 94.0.992.9	24-Sep-2021 94.0.992.31	24-Sep-2021 94.0.992.31
95	Released Version	28-Sep-2021 95.0.1020.9	21-Oct-2021 95.0.1020.30	Not applicable
96	Released Version	01-Nov-2021 96.0.1054.8	19-Nov-2021 96.0.1054.29	19-Nov-2021 96.0.1054.29
97	Released Version	01-Dec-2021 97.0.1072.21	06-Jan-2022 97.0.1072.55	Not applicable
98	Released Version	14-Jan-2022 98.0.1108.23	03-Feb-2022 98.0.1108.43	03-Feb-2022 98.0.1108.43
99	Released Version	09-Feb-2022 99.0.1150.11	03-Mar-2022 99.0.1150.30	Not applicable
100	Released Version	17-Mar-2022 100.0.1185.10	01-Apr-2022 100.0.1185.29	01-Apr-2022 100.0.1185.29
101	Released Version	08-Apr-2022 101.0.1210.10	28-Apr-2022 101.0.1210.32	Not applicable
102	Released Version	10-May-2022 102.0.1245.7	31-May-2022 102.0.1245.30	31-May-2022 102.0.1245.30
103	Released Version	02-Jun-2022 103.0.1264.13	23-Jun-2022 103.0.1264.37	Not applicable
104	Released Version	07-Jul-2022 104.0.1293.14	05-Aug-2022 104.0.1293.47	05-Aug-2022 104.0.1293.47
105	Released Version	16-Aug-2022 105.0.1343.7	01-Sep-2022 105.0.1343.25	Not applicable
106	Released Version	15-Sep-2022 106.0.1370.15	03-Oct-2022 106.0.1370.34	03-Oct-2022 106.0.1370.34
107	Released Version	13-Oct-2022 107.0.1418.8	27-Oct-2022 107.0.1418.24	Not applicable
108	Target release	Week of 01-Nov-2022	Week of 01-Dec-2022	Week of 01-Dec-2022
109	Target release	Week of 06-Dec-2022	Week of 12-Jan-2023	Not applicable
110	Target release	Week of 18-Jan-2023	Week of 09-Feb-2023	Week of 09-Feb-2023

Release process

The trigger for Beta and Stable major releases is an equivalent Chromium release.

Progressive rollouts

The date reference (Released/Release week) for the Stable channel references the beginning of the progressive rollout.

We use a progressive rollout model, which means that new release availability for any given device could be staggered over upcoming days. For more information, see Progressive rollouts for Microsoft Edge Stable Channel.

See also

- Microsoft Edge Enterprise landing page
- Microsoft Edge channels
- Channel downloads

Release notes for Microsoft Edge Security Updates

11/1/2022 • 19 minutes to read • Edit Online

These release notes provide information about security fixes that are included in updates to Microsoft Edge Stable channel.

October 31, 2022

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 107.0.1418.26)**. This update contains a fix for CVE-2022-3723, which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

Microsoft has also updated **Microsoft Edge Stable Channel (Version 106.0.1370.61)**, which contains the fix to CVE-2022-3723.

> **NOTE**
> It's worth highlighting that Microsoft Edge's enhanced security mode feature mitigates this vulnerability. You can opt-in into this security feature and have peace of mind that Microsoft Edge is protecting you against this exploit.

October 27, 2022

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 107.0.1418.24)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

October 14, 2022

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 106.0.1370.47)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

October 3, 2022

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 106.0.1370.34)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

This update contains the following Microsoft Edge-specific update:

- CVE-2022-41035

September 15, 2022

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 105.0.1343.42)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

September 2, 2022

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 105.0.1343.27)**. This update

contains a fix for CVE-2022-3075, which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

> **NOTE**
> Extended Stable channel has also been updated to 104.0.1293.81, which contains the fix.

September 1, 2022

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 105.0.1343.25)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide

This update contains the following Microsoft Edge-specific update:

- CVE-2022-38012

August 19, 2022

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 104.0.1293.63)**. This update contains a fix for CVE-2022-2856, which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

August 17, 2022

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 104.0.1293.60)**. This update contains a fix for CVE-2022-2856, which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

August 5, 2022

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 104.0.1293.47)**. For more information, see the Security Update Guide.

This update contains the following Microsoft Edge-specific updates:

- CVE-2022-33636
- CVE-2022-33649
- CVE-2022-35796

July 22, 2022

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 103.0.1264.71)**. For more information, see the Security Update Guide.

July 6, 2022

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 103.0.1264.49)**, which incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2022-2294, that has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

June 30, 2022

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 103.0.1264.44)**. For more information, see the Security Update Guide.

This update contains the following Microsoft Edge-specific update:

- CVE-2022-33680

June 23, 2022

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 103.0.1264.37)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

This update contains the following Microsoft Edge-specific updates:

- CVE-2022-30192
- CVE-2022-33638
- CVE-2022-33639

June 13, 2022

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 102.0.1245.41)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

June 9, 2022

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 102.0.1245.39)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

This update contains the following Microsoft Edge-specific update:

- CVE-2022-22021

May 31, 2022

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 102.0.1245.30)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

This update contains the following Microsoft Edge-specific updates:

- CVE-2022-30128
- CVE-2022-30127
- CVE-2022-26905

May 13, 2022

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 101.0.1210.47)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

April 28, 2022

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 101.0.1210.32)**, which

incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

This update also contains the following Microsoft Edge-specific update:

- CVE-2022-29146
- CVE-2022-29147

April 15, 2022

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 100.0.1185.44)**, which incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2022-1364, which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

This update also contains the following Microsoft Edge-specific update:

- CVE-2022-29144

April 7, 2022

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 100.0.1185.36)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

April 1, 2022

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 100.0.1185.29)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

This update contains the following Microsoft Edge-specific updates:

- CVE-2022-24523
- CVE-2022-24475
- CVE-2022-26891
- CVE-2022-26895
- CVE-2022-26894
- CVE-2022-26900
- CVE-2022-26908
- CVE-2022-26909
- CVE-2022-26912

March 26, 2022

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 99.0.1150.55)**, which incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2022-1096, which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

March 17, 2022

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 99.0.1150.46)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security

Update Guide.

This update contains the following Microsoft Edge-specific update:

- CVE-2022-26899

March 3, 2022

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 99.0.1150.30)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

February 16, 2022

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 98.0.1108.55)**, which incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2022-0609, which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

February 10, 2022

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 98.0.1108.50)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

This update contains the following Microsoft Edge-specific updates:

- CVE-2022-23264

February 3, 2022

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 98.0.1108.43)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

This update contains the following Microsoft Edge-specific updates:

- CVE-2022-23261
- CVE-2022-23262
- CVE-2022-23263

January 20, 2022

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 97.0.1072.69)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

This update contains the following Microsoft Edge-specific update:

- CVE-2022-23258

January 6, 2022

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 97.0.1072.55)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

This update contains the following Microsoft Edge-specific updates:

- CVE-2022-21954
- CVE-2022-21929
- CVE-2022-21930
- CVE-2022-21931
- CVE-2022-21970

December 14, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 96.0.1054.57)**, which incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2021-4102, that has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

December 10, 2021

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 96.0.1054.53)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

November 19, 2021

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 96.0.1054.29)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

This update contains the following Microsoft Edge-specific updates:

- CVE-2021-43220
- CVE-2021-42308
- CVE-2021-43221

October 29, 2021

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 95.0.1020.40)**, which incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2021-38000 and CVE-2021-38003 which have been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

October 21, 2021

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 95.0.1020.30)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide

October 11, 2021

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 94.0.992.47)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide

October 1, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 94.0.992.38)**, which

incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2021-37975 and CVE-2021-37976 which have been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

September 24, 2021

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 94.0.992.31)**, which incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2021-37973 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide

September 16, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 93.0.961.52)**, which incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2021-30633 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

September 11, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 93.0.961.47)**, which incorporates the latest Security Updates of the Chromium project.This update contains a fix for CVE-2021-30632 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide

September 9, 2021

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 93.0.961.44)** which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide

This update contains the following Microsoft Edge-specific update:

- CVE-2021-38669

September 2, 2021

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 93.0.961.38)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide

This update contains the following Microsoft Edge-specific update:

- CVE-2021-36930
- CVE-2021-26436
- CVE-2021-26439
- CVE-2021-38641
- CVE-2021-38642

August 19, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 92.0.902.78)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide

August 5, 2021

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 92.0.902.67)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide

July 22, 2021

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 92.0.902.55)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide

This update contains the following Microsoft Edge-specific update:

- CVE-2021-36928
- CVE-2021-36929
- CVE-2021-36931

July 19, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 91.0.864.71)**, which incorporates the latest Security Updates of the Chromium project. This update containsa fix for CVE-2021-30563 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

June 24, 2021

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 91.0.864.59)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide

This update contains the following Microsoft Edge-specific update:

- CVE-2021-34506
- CVE-2021-34475

June 18, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 91.0.864.54)**, which incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2021-30554 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

June 11, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (version 91.0.864.48)**, which incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2021-30551 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

June 03, 2021

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 91.0.864.41)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

This update contains the following Microsoft Edge-specific update:

- CVE-2021-33741

May 27, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 91.0.864.37)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

This update contains the following Microsoft Edge-specific update:

- CVE-2021-31982
- CVE-2021-31937

May 13, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 90.0.818.62)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

April 29, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 90.0.818.51)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

April 22, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 90.0.818.46)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

April 16, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 90.0.818.41)**, which incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2021-21224 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

April 15, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 90.0.818.39)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

April 14, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 89.0.774.77)**, which incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2021-21206 and CVE-2021-21220 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

April 1, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 89.0.774.68)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

March 13, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 89.0.774.54)**, which incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2021-21193 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

March 4, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 89.0.774.45)**, which incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2021-21166 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

February 17, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 88.0.705.74)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

February 5, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 88.0.705.63)**, which incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2021-21148 which has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

February 4, 2021

Microsoft has released the latest**Microsoft Edge Stable Channel (Version 88.0.705.62)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

This update contains the following Microsoft Edge-specific update:

- CVE-2021-24113

January 21, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 88.0.705.50)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

January 7, 2021

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 87.0.664.75)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

December 7, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 87.0.664.57)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

November 19, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 87.0.664.41)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

November 13, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 86.0.622.69)**, which incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2020-16013 and CVE-2020-16017, that have been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

November 11, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 86.0.622.68)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

November 4, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 86.0.622.63)**, which incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2020-16009, that has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

October 22, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 86.0.622.51)**, which incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2020-15999, that has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

October 9, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 86.0.622.38)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

September 23, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 85.0.564.63)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

September 9, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 85.0.564.51)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

August 27, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 85.0.564.41)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security

Update Guide.

August 20, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 84.0.522.63)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

August 11, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 84.0.522.59)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

July 29, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 84.0.522.49)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

July 16, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 84.0.522.40)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

This update contains the following Microsoft Edge-specific update:

- CVE-2020-1341

June 24, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 83.0.478.56)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

June 17, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 83.0.478.54)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

June 4, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 83.0.478.45)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

May 21, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 83.0.478.37)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

This update contains the following Microsoft Edge-specific update:

- CVE-2020-1195

May 7, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 81.0.416.72)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

April 29, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 81.0.416.68)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

April 23, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 81.0.416.64)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

April 17, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 81.0.416.58)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

April 13, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 81.0.416.53)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

April 1, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 80.0.361.109)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

March 19, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 80.0.361.69)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

March 4, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 80.0.361.66)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

February 25, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 80.0.361.62)**, which incorporates the latest Security Updates of the Chromium project. This update contains a fix for CVE-2020-6418,

that has been reported by the Chromium team as having an exploit in the wild. For more information, see the Security Update Guide.

February 20, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 80.0.361.57)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

February 7, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 80.0.361.48)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

January 17, 2020

Microsoft has released the latest **Microsoft Edge Stable Channel (Version 79.0.309.68)**, which incorporates the latest Security Updates of the Chromium project. For more information, see the Security Update Guide.

See also

- Microsoft Edge Enterprise landing page

Microsoft Edge supported Operating Systems

11/1/2022 • 3 minutes to read • Edit Online

This article describes the supported operating systems that apply to Microsoft Edge.

> **NOTE**
> This article applies to the Microsoft Edge versions 77 and higher for the desktop.

Supported Operating Systems for Microsoft Edge

> **NOTE**
> Product functionality and feature availability may vary on older operating systems. To ensure that Microsoft Edge installs correctly, use the latest version of any operating system specified below. This guidance includes the latest cumulative update, as applicable.

Microsoft Edge follows the Modern Lifecycle Policy and is supported on the following operating systems.

Windows Client

- Windows 7 **
- Windows 8.1
- Windows 10 SAC 1709 and later ***
- Windows 10 Enterprise 2015 LTSC
- Windows 10 Enterprise 2016 LTSC
- Windows 10 Enterprise 2019 LTSC
- Windows 10 Enterprise 2021 LTSC
- Windows 10 Enterprise multi-session
- Windows 10 IoT Enterprise SAC ****
- Windows 10 IoT Enterprise 2019 LTSC ****

Windows Server

- Windows Server 2008 R2 **
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016 (LTSC)
- Windows Server 2019 (LTSC)
- Windows Server 2022 (LTSC)
- Windows Server (SAC)

IMPORTANT

** We will continue to support Microsoft Edge on Windows 7 and on Windows Server 2008 R2 until January 15, 2023. These operating systems are out of support and Microsoft recommends you move to a supported operating system such as Windows 10. While Microsoft Edge helps keep you more secure on the web, your PC may still be vulnerable to security risks. In order for IE mode to be supported on these operating systems the devices will need to have the Extended Security Updates for Windows 7. Without the Windows 7 Extended Security updates Internet Explorer functionality will be vulnerable to security risks. Additionally, IE mode functionality may cease to work without the continued servicing through the extended security updates. Microsoft Edge on Windows 7 can be updated using the built-in auto update engine or using Configuration Manager and WSUS.

*** In the same fashion as above, for Windows 10 SAC releases that are out of support but Microsoft Edge is supported it is recommended to upgrade to a supported Win10 SAC release as soon as possible to remain secure. Microsoft Edge being supported in this state should be considered a temporary bridge to getting to a supported OS state.

**** The Microsoft Edge OPK is available on MOO for IoT OEMs to preinstall and distribute as part of their Windows 10 IoT Enterprise based solution.

macOS

- High Sierra (10.13) and later

iOS

Microsoft Edge for iPad® and iPhone® requires iOS 11.0 or later. Microsoft Edge for iPad Pro™ requires iOS 11.0 or later. Microsoft Edge is supported on the two most recent versions of iOS. When a new version of iOS is released, the Microsoft Edge Operating System requirement becomes the then-current two most recent versions: the new version of iOS and the previous version.

Android

Microsoft Edge for Android can be installed on tablets and phones that meet the following criteria: devices running Android KitKat 4.4 or later with an ARM-based processor.

Apple Silicon Macs

Microsoft Edge native support as of Stable version 88 for Apple Silicon Macs.

Linux

Preview builds are available for Linux. For any issues related to Microsoft Edge on Linux, either as a Developer or as an Enterprise, please file feedback directly through the browser or by utilizing our TechCommunity forums https://techcommunity.microsoft.com/t5/microsoft-edge-insider/ct-p/MicrosoftEdgeInsider. Enterprise support for Microsoft Edge on Linux is coming at a later time.

Chromebooks

Microsoft Edge does not support Chromebooks.

Recent changes

- **12/17/2020** - Microsoft Edge support on Windows 7 and Windows Server 2008 R2 extended to January 15, 2022.
- **01/28/2021** - Microsoft Edge support for Apple Silicon Macs.
- **11/05/2021** - Microsoft Edge support on Windows 7 and Windows Server 2008 R2 extended through January 15, 2023 for critical security and stability updates.

See also

- Microsoft Edge Enterprise landing page

- Microsoft Modern Lifecycle Policy
- Extended Security Updates for Windows 7

Microsoft Edge Lifecycle Policy

11/1/2022 • 2 minutes to read • Edit Online

This article describes the lifecycle policy that applies to Microsoft Edge.

> **NOTE**
> This article applies to Microsoft Edge versions 77 and higher.

> **NOTE**
> Starting with Stable channel version 94, Microsoft Edge moved to a 4-week major release cycle cadence. However, we recognize that enterprise customers who manage complex environments need more time to plan and test Microsoft Edge updates. To help our enterprise customers who need an extended timeline to manage updates, Microsoft Edge offers an **Extended Stable option aligned to a longer, 8-week major release cycle.** This release option is only available for customers with managed environments. Refer to our announcement blog post

Overview of the lifecycle policy for Microsoft Edge

Microsoft Edge features more frequent and more flexible updating capabilities. Because browser releases aren't bound to the Windows major releases, it's necessary to have the governing lifecycle policy updated to reflect this decoupling. Going forward, Microsoft Edge will follow the Modern Lifecycle Policy. Security updates and servicing updates are only available on the latest Stable channel release and the latest Beta channel release. If you use older releases of Microsoft Edge, it's likely that you'll miss the latest quality and security updates. Using older versions isn't recommended. Assisted Support is available as described in the following section.

Service and assisted support timeline

Starting with Stable channel version 94, Microsoft Edge moved to a 4-week major release cycle cadence. We continue to provide Assisted Support for the most recent three Stable channel releases and the latest Beta channel release. The effective assisted support duration for a Stable channel release is approximately 12 weeks.

We recognize that enterprise customers who manage complex environments need more time to plan and test Microsoft Edge updates. To help our enterprise customers who need an extended timeline to manage updates, Microsoft Edge offers an **Extended Stable option aligned to a longer, 8-week major release cycle**. Assisted Support is available for the most recent two Extended Stable channel releases. The effective assisted support duration for an Extended Stable channel release is approximately 16 weeks. The following table summarizes the support options for different Microsoft Edge releases.

RELEASE OPTION	MAJOR VERSION RELEASE SUPPORTED	MAJOR VERSION RELEASE SERVICED	SUPPORT COVERAGE ACROSS RELEASES	SERVICING COVERAGE
Daily “Canary”	None	None	None	None
Weekly “Dev”	None	None	None	None
4-week “Beta”	Current	Current	4 weeks	4 weeks

RELEASE OPTION	MAJOR VERSION RELEASE SUPPORTED	MAJOR VERSION RELEASE SERVICED	SUPPORT COVERAGE ACROSS RELEASES	SERVICING COVERAGE
`4`-week "Stable"	Current and `2` previous	Current	`12` weeks	`4` weeks
`8`-week "Extended Stable"	Current and `1` previous	Current	`16` weeks	`8` weeks

See also

- Microsoft Edge Enterprise landing page
- Microsoft Edge documentation
- Microsoft Modern Lifecycle Policy
- Microsoft Edge Supported Operating Systems

Microsoft Edge language support

11/1/2022 • 3 minutes to read • Edit Online

This article shows how you can use Microsoft Edge settings to add a supported language to the browser. Microsoft Edge supports 84 display languages on Windows and 81 display languages on macOS.

> **NOTE**
> This article applies to Microsoft Edge version 78 or later.

Add a supported language to Microsoft Edge

Use the following steps to see the list of supported languages and then add a language to Microsoft Edge.

1. On the browser menu bar, click the **Settings and more** icon (...) or type **Alt+F** to open the "Settings and more" menu.
2. Under **Settings**, click **Languages**.
3. Under **Languages**, click **Add languages** to see the list of languages you can add.
4. In the **Add languages** list, you can search for a language (**Search languages**) or use the scroll bar to find the language you want to add.
5. When you find the language, select the checkbox for the language and then click **Add**. The language you added will appear at the bottom of the list of **Preferred languages** that are already set for Microsoft Edge. Websites you visit will appear in the first language in the list that they support.

Change preferred languages

You can reorder your language preferences, get Microsoft Edge to offer translations, and see Microsoft Edge in a specific language. To change a language setting, click the ellipsis (...) next to the language to open for "More actions". Depending on the language, you will see one or more of the following options:

- Display Microsoft Edge in this language.
  - On Windows, select this box and then click **Restart**.
  - On macOS, Microsoft Edge is displayed in the preferred language of your system. You can change the language in **System Preferences>Language & Region**. Restart Microsoft Edge.
- Offer to translate pages in this language. This option is only available if you enable the **Offer to translate pages that aren't in a language you read**.
- Move to the top
- Move up
- Remove

> **NOTE**
> You can also set up spellcheck options (**Check Spelling**) based on your preferred language settings.

Foreign language translator extension

In addition to using a foreign language in the browser, you can use the Translator for Microsoft Edge extension to translate foreign language web pages and text selections for more than 60 languages.

NOTE

If the translator extension doesn't work after installation, restart Microsoft Edge. If the extension still doesn't work, provide feedback through the Feedback Hub.

Supported display languages

The following table lists the display languages that are supported by Microsoft Edge.

NOTE

Languages that aren't supported by Microsoft Edge on macOS are indicated by an asterisk (*) after the country/region.

LANGUAGE	COUNTRY/REGION	CODE
Afrikaans	South Africa	af
Albanian	Albania	sq
Amharic	Ethiopia	am
Arabic	Saudi Arabia	ar
Assamese	India	as
Azerbaijani	Azerbaijan, Latin	az
Bangla	India*	bn-IN
Basque	Basque	eu
Bosnian	Bosnia and Herzegovina, Latin	bs
Bulgarian	Bulgaria	bg
Catalan	Catalan	ca
Chinese	China, Simplified	zh-CN
	Taiwan, Traditional	zh-TW
Croatian	Croatia	hr
Czech	Czech Republic	cs
Danish	Denmark	da
Dutch	Netherlands	nl
English	United Kingdom	en-GB

LANGUAGE	COUNTRY/REGION	CODE
	United States	en
Estonian	Estonia	et
Filipino	Philippines	fil
Finnish	Finland	fi
French	Canada	fr-CA
	France	fr
Galician	Galician	gl
Georgian	Georgia	ka
German	Germany	de
Greek	Greece	el
Gujarati	India	gu
Hebrew	Israel	he
Hindi	India	hi
Hungarian	Hungary	hu
Icelandic	Iceland	is
Indonesian	Indonesia	id
Irish	Ireland	ga
Italian	Italy	it
Japanese	Japan	ja
Kannada	India	kn
Kazakh	Kazakhstan	kk
Khmer	Cambodia	km
Konkani	India	kok
Korean	Korea	ko
Lao	Laos P.D.R.	lo

LANGUAGE	COUNTRY/REGION	CODE
Latvian	Latvia	lv
Lithuanian	Lithuania	lt
Luxembourgish	Luxembourg	lb
Macedonian	North Macedonia	mk
Malay	Malaysia	ms
Malayalam	India	ml
Maltese	Malta	mt
Maori	New Zealand	mi
Marathi	India	mr
Nepali	Nepal	ne
Norwegian	Norway, Bokmål	nb
	Norway, Nynorsk	nn
Odia	India	or
Persian	Iran	fa
Polish	Poland	pl
Portuguese	Brazil	pt-BR
	Portugal	pt-PT
Punjabi	India	pa
Quechua	Peru	quz
Romanian	Romania	ro
Russian	Russia	ru
Scottish Gaelic	United Kingdom	gd
Serbian	Bosnia and Herzegovina, Cyrillic*	sr-Cyrl-BA
	Serbia, Cyrillic	sr-Cyrl-RS
	Serbia, Latin	sr-Latn-RS

LANGUAGE	COUNTRY/REGION	CODE
Slovak	Slovakia	sk
Slovenian	Slovenia	sl
Spanish	Mexico	es-MX
	Spain, International Sort	es
Swedish	Sweden	sv
Tamil	India	ta
Tatar	Russia	tt
Telugu	India	te
Thai	Thailand	th
Turkish	Turkey	tr
Ukrainian	Ukraine	uk
Urdu	Islamic Republic of Pakistan	ur
Uyghur	PRC	ug
Valencian	Spain*	ca-Es-VALENCIA
Vietnamese	Vietnam	vi
Welsh	United Kingdom	cy

See also

- Microsoft Edge documentation
- Microsoft Edge Enterprise landing page

Windows updates to support the next version of Microsoft Edge

11/1/2022 • 2 minutes to read • Edit Online

This article describes how Windows will be updated to support the next version of Microsoft Edge

IMPORTANT

Refer to the Microsoft Edge product team blog post about Microsoft Edge Legacy end of service.

NOTE

This article applies to the Microsoft Edge Stable channel.

Microsoft Edge and the Windows release cycle

The next version of Microsoft Edge features more frequent and more flexible updating capabilities. Because browser releases aren't bound to the Windows major releases, changes will be made to the operating system to ensure that the next version of Microsoft Edge fits seamlessly into Windows. As a result, feature updates will be released on a 4-week cycle (approximately). Security and compatibility updates will be shipped as needed.

Updates and the user experience

Updates won't change the user experience until the Stable channel of the next version of Microsoft Edge is installed. Installing Microsoft Edge Beta, Dev, or Canary won't trigger any changes in Windows. These browser releases will be installed alongside existing browsers.

When all the updates are applied AND the Stable channel of the next version of Microsoft Edge is installed at the system-level, the following changes will take effect on the system:

- All start menu pins, tiles, and shortcuts for the current version of Microsoft Edge will migrate to the next version of Microsoft Edge.
- All taskbar pins and shortcuts for the current version of Microsoft Edge will migrate to the next version of Microsoft Edge.
- The next version of Microsoft Edge will be pinned to the taskbar. If the current version of Microsoft Edge is already pinned, it will be replaced.
- The next version of Microsoft Edge will add a shortcut to the desktop. If the current version of Microsoft Edge already has a shortcut, it will be replaced.
- Most protocols that Microsoft Edge handles by default will be migrated to the next version of Microsoft Edge.
- Current Microsoft Edge will be hidden from all UX surfaces in the OS, including settings, all apps, and any file or protocol support dialogs.
- All attempts to launch the current version of Microsoft Edge will redirect to the next version of Microsoft Edge.

> **NOTE**
> User-level installs won't trigger the preceding behaviors.

Along with the previous changes, there are changes that will happen regardless of whether the Stable channel of the next version of Microsoft Edge is installed.

- Microsoft Edge will de-register for the books and XML protocols that the next version of Microsoft Edge doesn't support. Users attempting to open these protocols will get a dialog that prompts them to choose a default app. Visit the Microsoft Store to see our recommendations for ebook readers.

Older versions of Windows

To deploy Microsoft Edge on a device running a Windows version older than Windows 10 RS4, use Configuration Manager, Microsoft Intune, or upgrade to a supported version of Windows 10. The following article lists the currently supported versions of Windows 10 and Windows 11.

- Supported versions of Windows client

> **NOTE**
> For Windows 10 RS4-20H1, deploy a Windows LCU from May 2021 or newer to get Microsoft Edge. For more information, see Windows 10 update history

> **IMPORTANT**
> If you need updates not listed here, please run Windows Update or contact your administrator.

See also

- Microsoft Edge Enterprise landing page
- Microsoft Edge documentation

Deploy Microsoft Edge with Windows 10 updates

11/1/2022 • 2 minutes to read • Edit Online

The article provides information for users who are deploying Microsoft Edge by using Windows 10 updates.

For Windows 10 release 20H2

Windows 10 20H2 and later include Microsoft Edge pre-installed as the default browser. However, version 84 of Microsoft Edge that shipped with Windows 10 20H2, and version 92 of Microsoft Edge that shipped with Windows 10 21H2, are now outdated. While Microsoft Edge will automatically update itself to a newer version after a user has logged on, since the timing of the update is dependant upon various factors, this can be unpredictable. For organizations that desire greater control and want to ensure that Microsoft Edge (Stable channel) is updated to the latest version before user sign-in, the following PowerShell command can be used to force a Microsoft Edge update during Windows OOBE.

```
Start-Process -FilePath "C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe" -argumentlist
"/silent /install appguid={56EB18F8-B008-4CBD-B6D2-8C97FE7E9062}&appname=Microsoft%20Edge&needsadmin=True"
```

If using Windows Autopilot, it's possible to wrap this script as an .intunewin file using the Microsoft Win32 content prep tool. It can then be set as a required app for the Enrollment Status Page (ESP) if desired.

> **NOTE**
> If you currently leverage policies such as Target Channel override or Target Version override to remain on an older version of Microsoft Edge, be aware that the above script will not take any policies into account, and will simply update to the latest version. By default, Microsoft Edge does not downgrade itself, including once such policies are later received.

For Windows 10 releases RS4 through 20H1

Windows Server Update Services (WSUS) has updates for each version of Windows 10 from RS4 through 20H1 that will remove the Microsoft Edge Legacy desktop app and replace it with Microsoft Edge. For more information, see this support article to find out which WSUS update is right for your Windows version.

For Windows 10 releases prior to RS4 (and Windows 7, 8.1, and earlier)

Windows updates to install Microsoft Edge aren't available for these versions. Consider other options for deploying Microsoft Edge to these devices such as Configuration Manager or Intune.

See also

- Microsoft Edge Enterprise landing page
- Plan your deployment of Microsoft Edge

Deploy to macOS with Jamf

11/1/2022 • 2 minutes to read • Edit Online

This article describes how to deploy Microsoft Edge for macOS using Jamf.

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

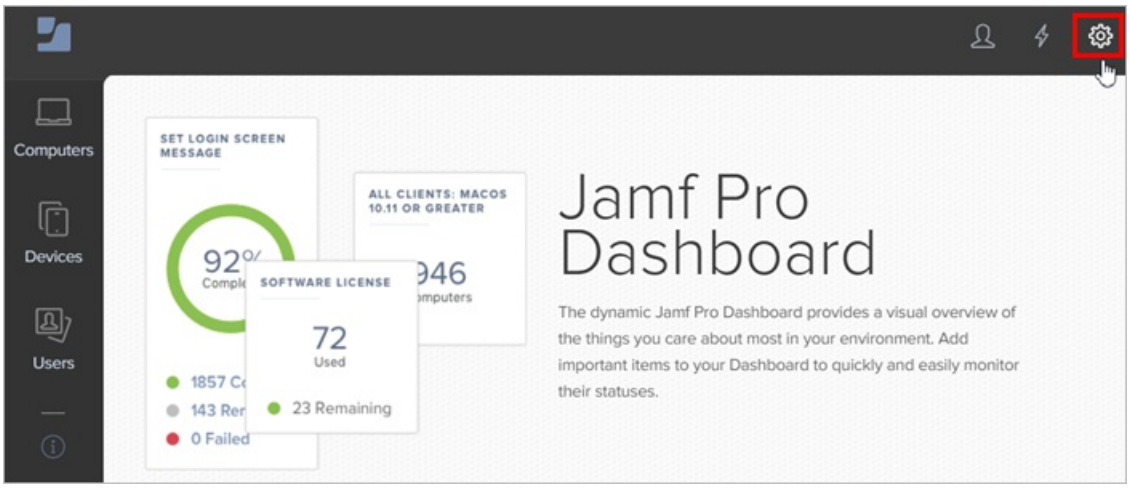
Prerequisites

Before you deploy Microsoft Edge, make sure you meet the following prerequisites:

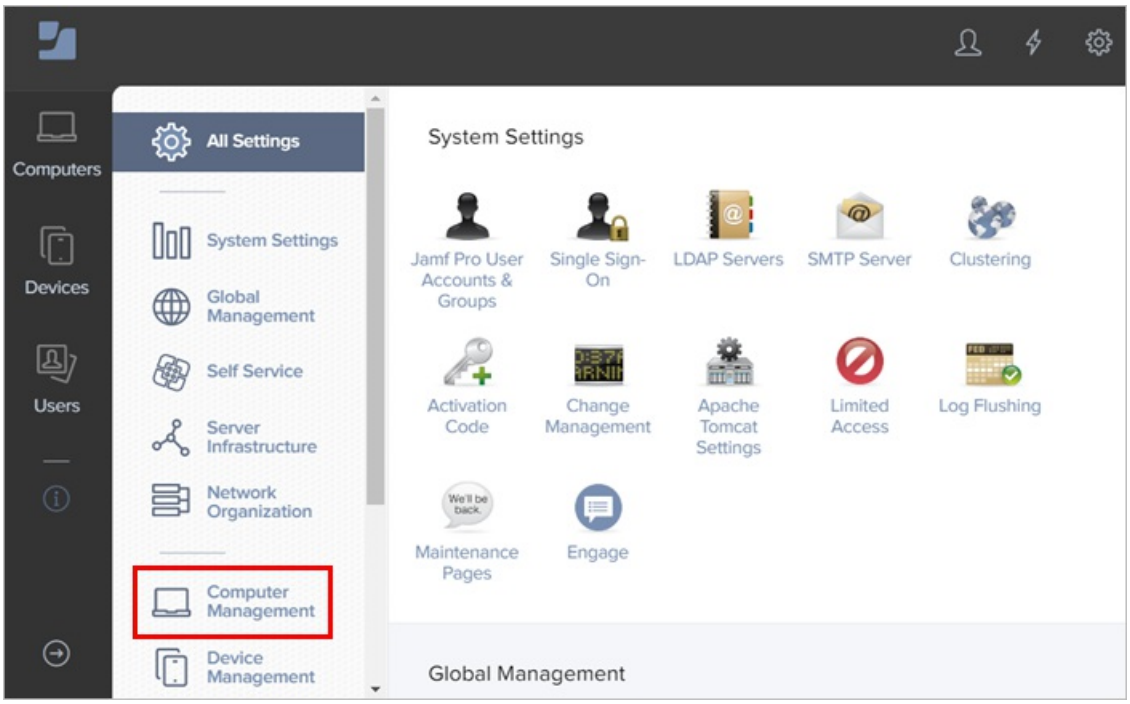
- The Microsoft Edge installation file, **MicrosoftEdgeDev-<version>.pkg** is in an accessible location on your network. You can download the Microsoft Edge Enterprise installation files from the Microsoft Edge Enterprise landing page.
- You have a Jamf Cloud account with the level of access and privileges needed to create and deploy installation files to computers.

To deploy Microsoft Edge using Jamf:

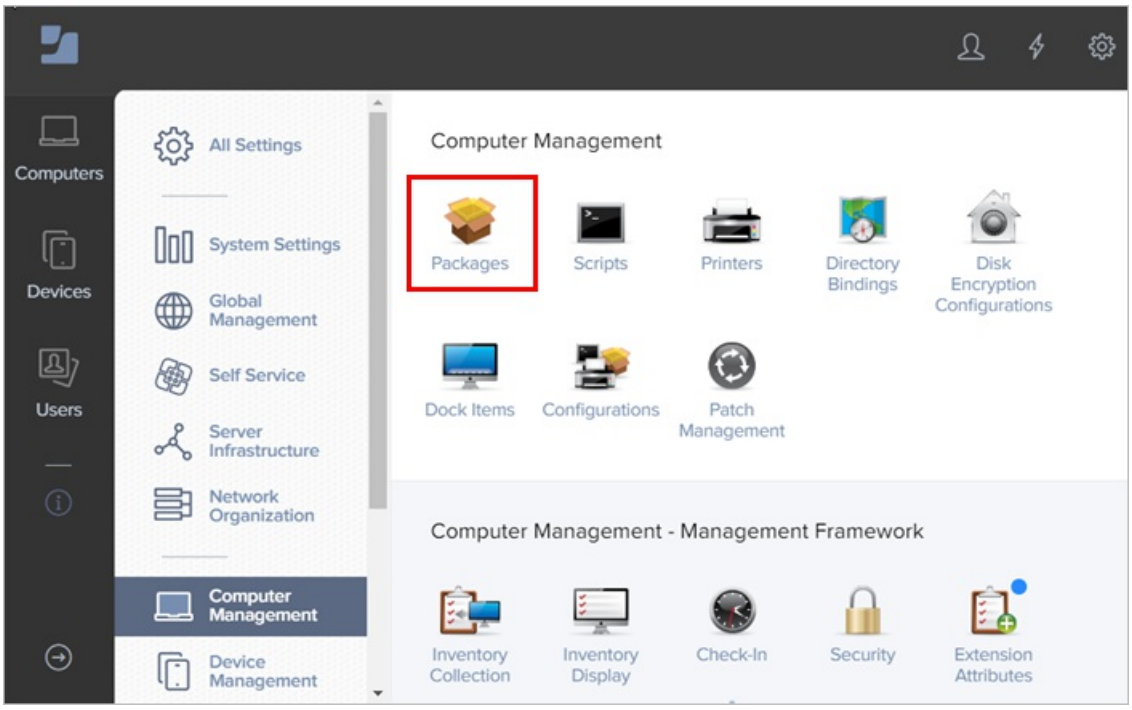
1. Sign on to Jamf and go to **All Settings**.


Computers
Devices
Users
SET LOGIN SCREEN MESSAGE
ALL CLIENTS: MACOS 10.11 OR GREATER
SOFTWARE LICENSE
72
Used
23 Remaining
0 Failed
Jamf Pro Dashboard
The dynamic Jamf Pro Dashboard provides a visual overview of the things you care about most in your environment. Add important items to your Dashboard to quickly and easily monitor their statuses.

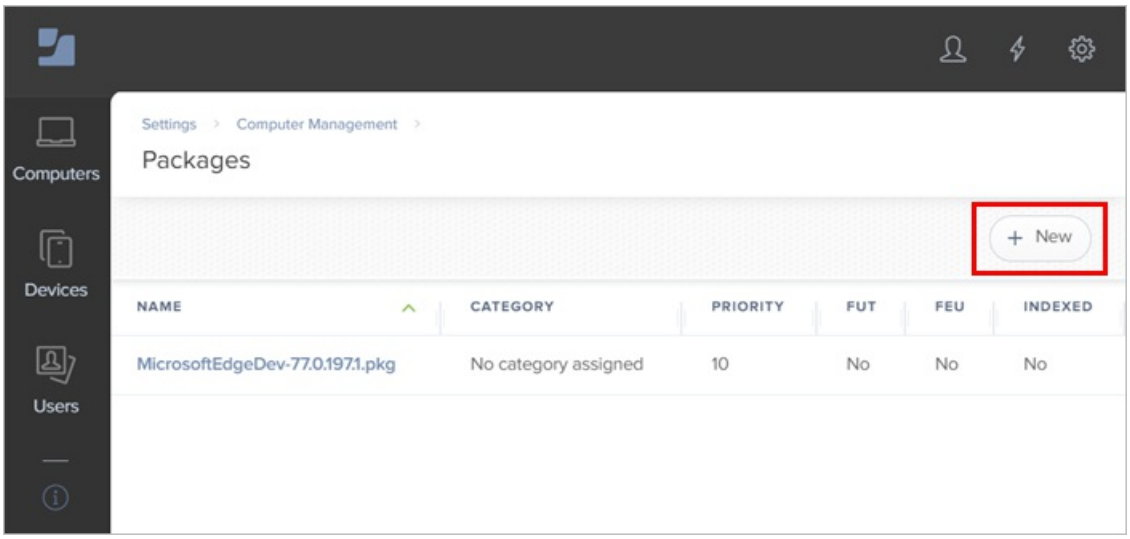
2. Under **All Settings**, click **Computer Management**.



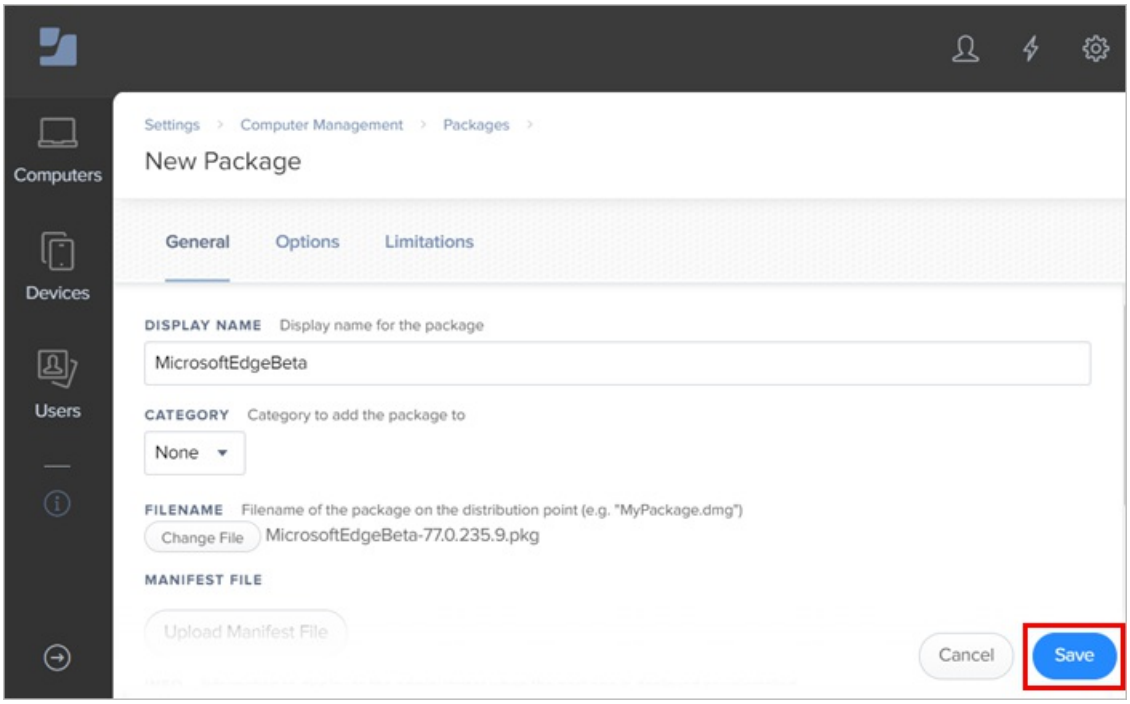
3. Under **Computer Management**, click **Packages**.



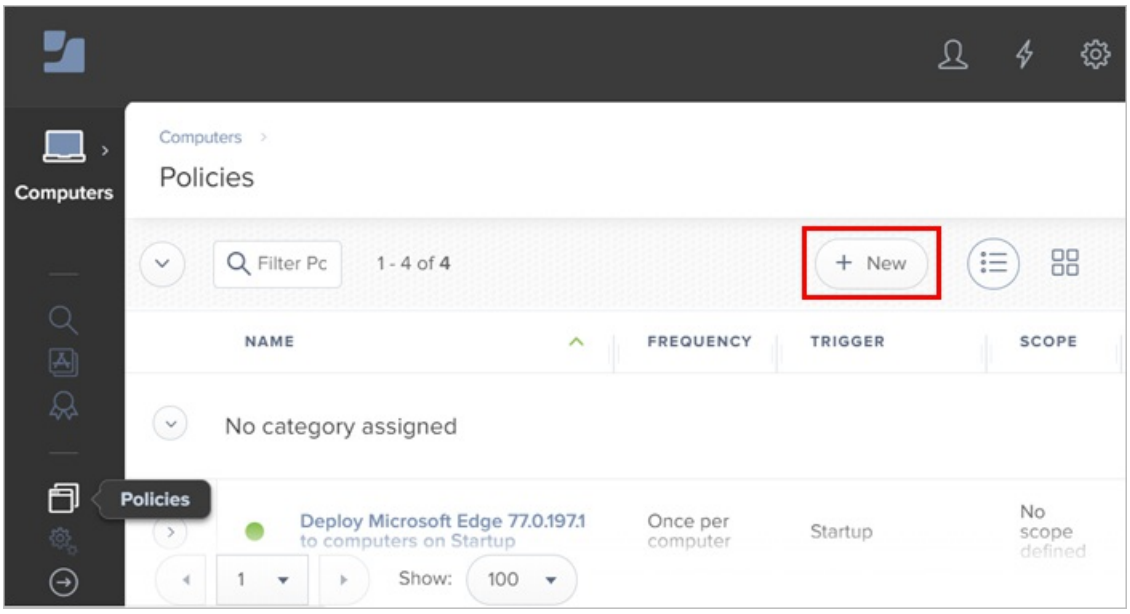
4. On the **Packages** page, click **+ New** to add a new package.



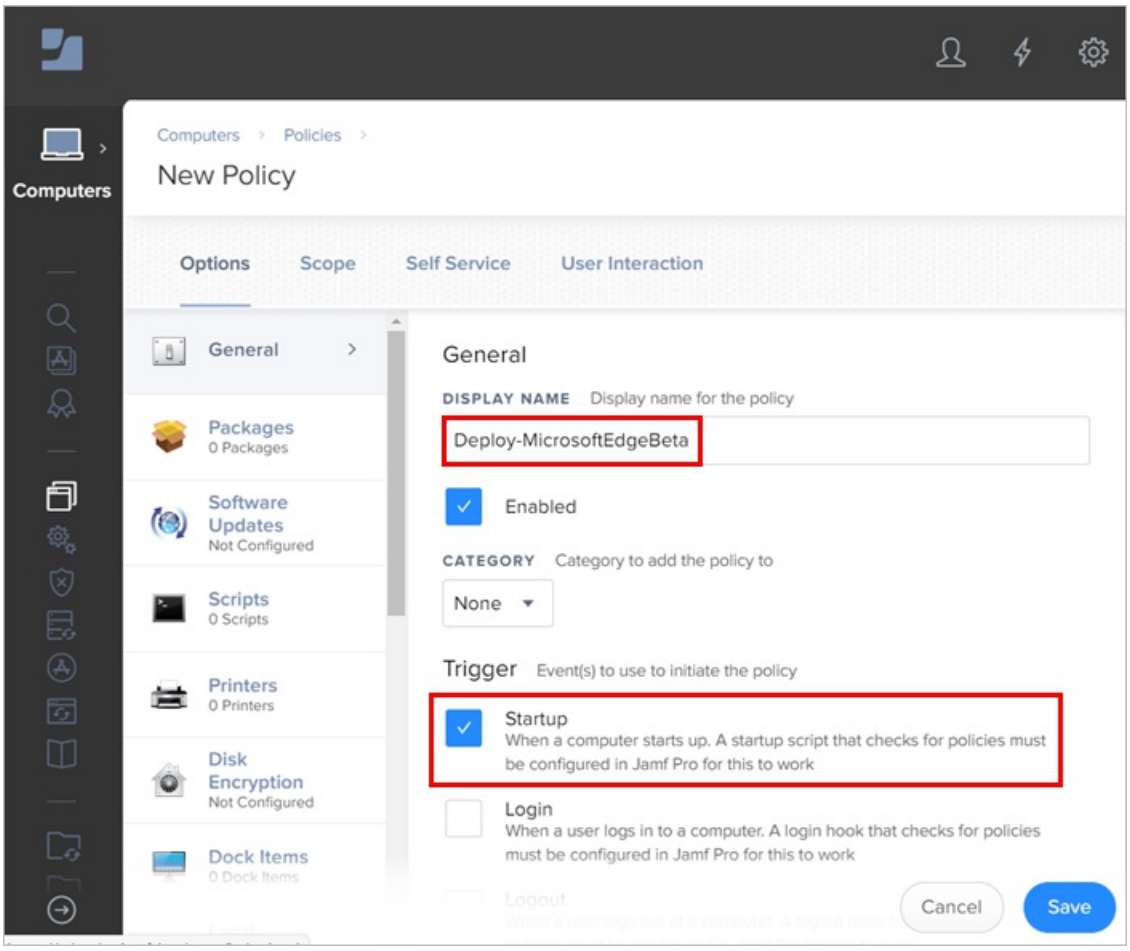
5. On the **New Package** page, enter the details about the package and then click **Save**. (For example, DISPLAY NAME, INFO, or NOTES.)



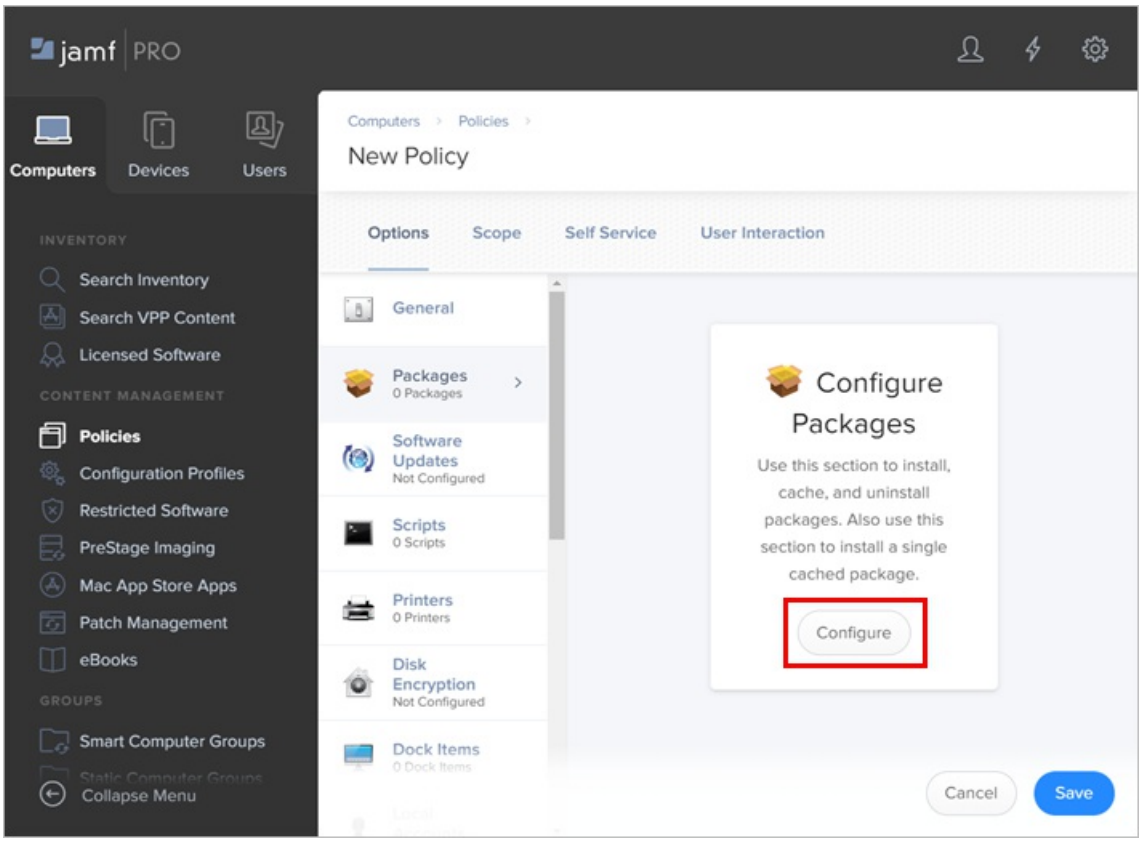
6. Select **Computers** on the menu bar, and then select **Policies** in the navigation bar.
7. Select **+ New** to display the **New Policy** pane.



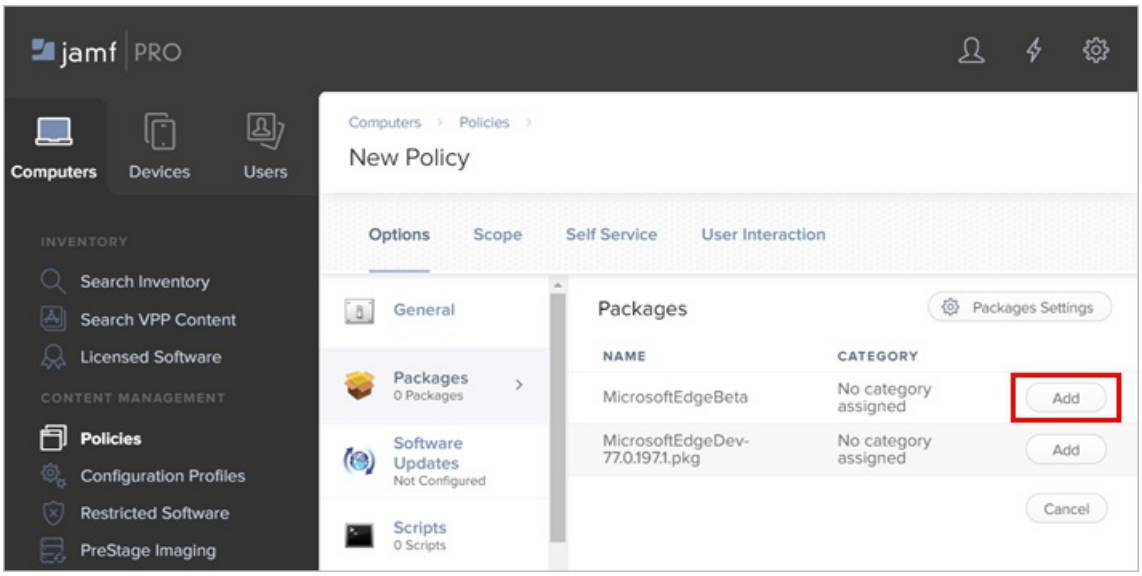
8. On the **Options** tab, select **General**.
   - Under **DISPLAY NAME**, enter the display name for the policy.
   - Under **Trigger**, select the event that will trigger the policy. (In the following example, the event is Startup.)



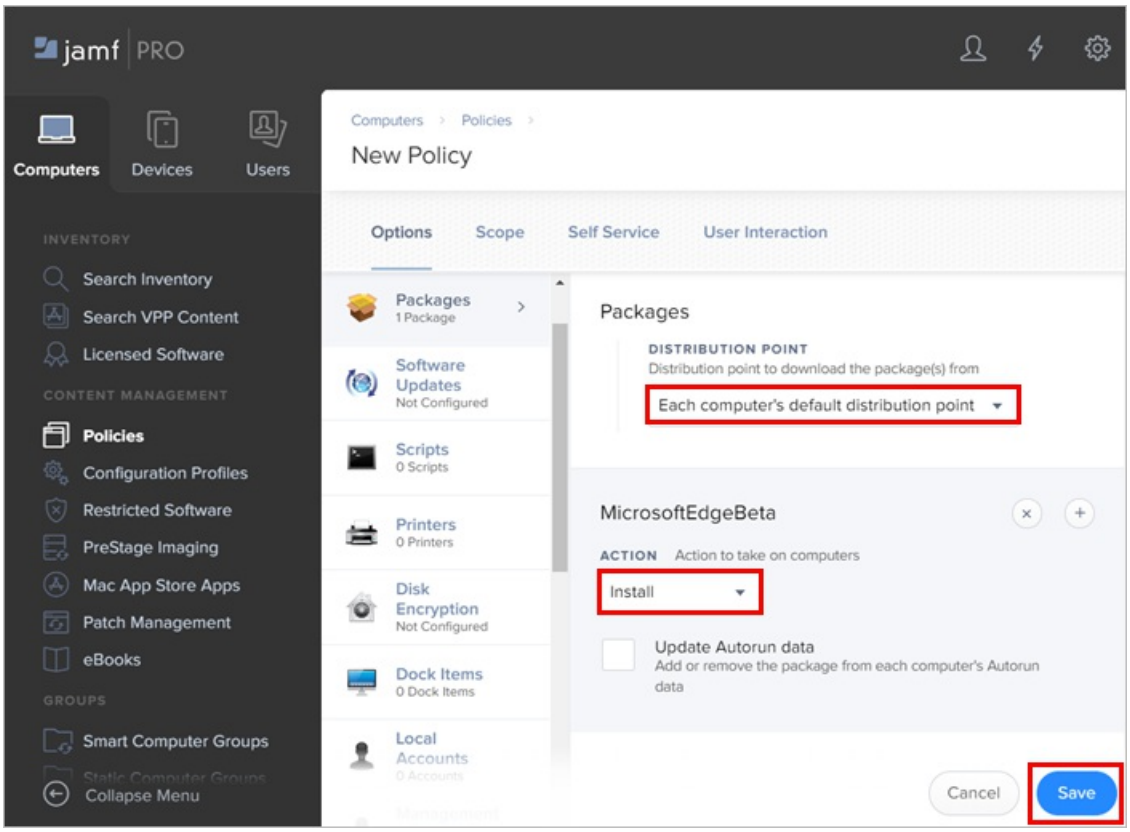
9. On the **Options** tab, click **Packages**.
10. On the **Configure Packages** popup, click **Configure**.



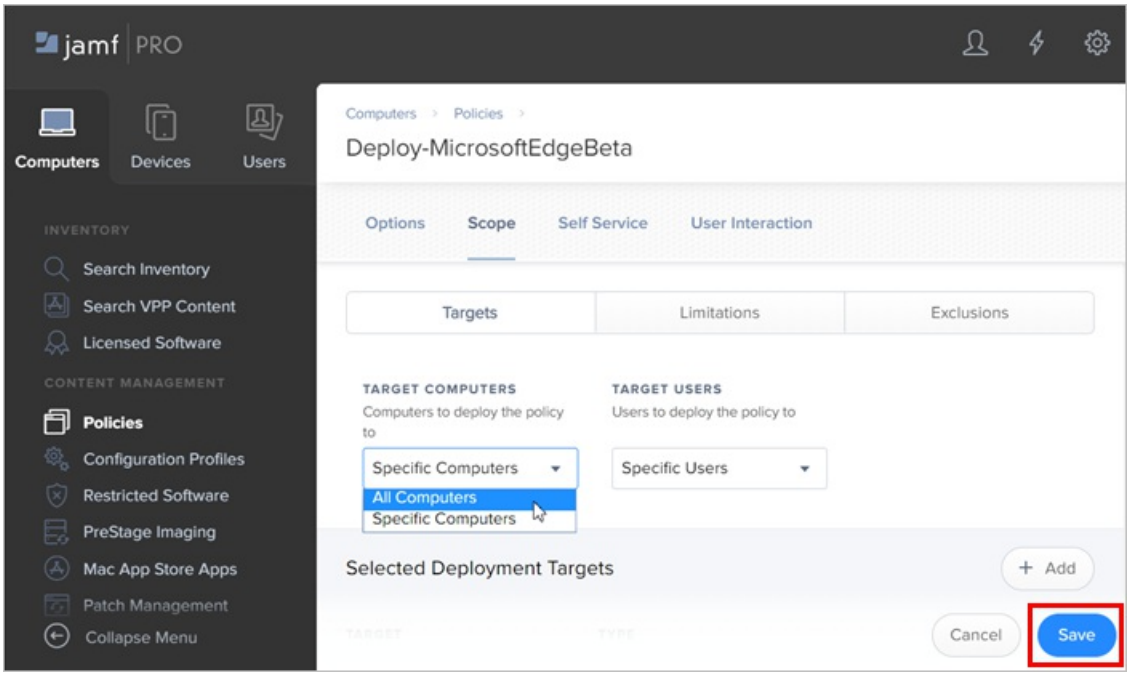
11. The package that you added shows on the **Packages** pane. Click **Add**. For this example, the package is "MicrosoftEdgeBeta" in the following screenshot.



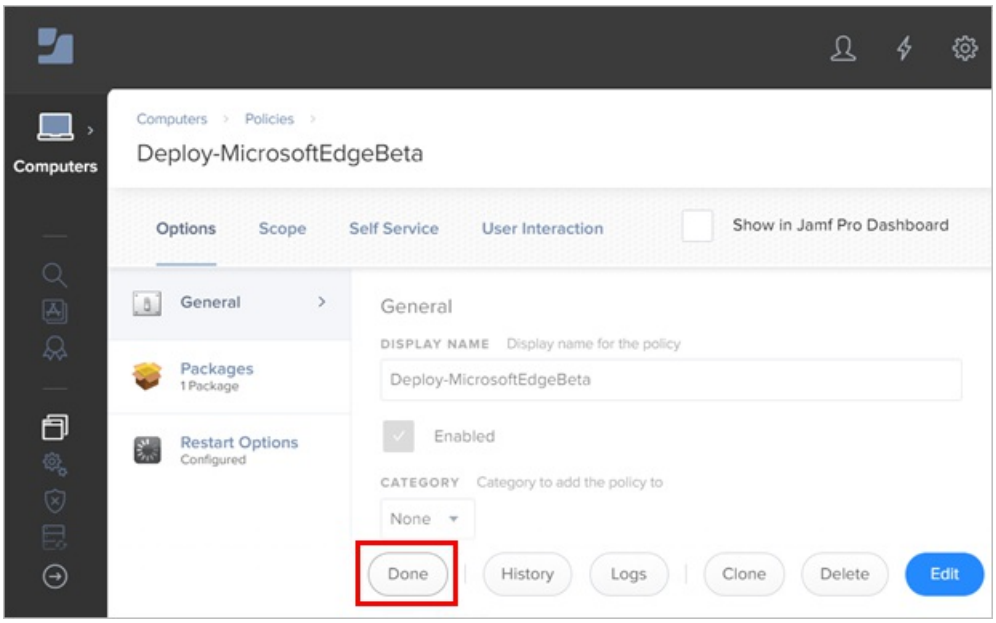
12. On the **New Policy** page, uUse the drop-down lists to select the **DISTRIBUTION POINT** and **ACTION** to take for the policy. Click **Save**. The following screenshot uses "Each computer's default distribution point" and "Install" as an example.



13. On the **New Policy** page, select the **Scope** tab. You can manage the scope of the deployment based on computers or users. For this example, select **All Computers** from the **TARGET COMPUTERS** drop-down list and then click **Save**.



14. At this point you can review the Microsoft Edge deployment policy. If the deployment options meet your requirements, click **Done**.



> **NOTE**
>
> You can return to a deployment policy at any time to change settings.

Congratulations! You've just finished configuring Jamf to deploy Microsoft Edge for macOS. When the trigger condition you defined is true, the package will get deployed to the computers you specified.

See also

- Microsoft Edge Enterprise landing page
- Jamf.com
- Integrate Jamf with Microsoft Intune

Configure Microsoft Edge policy settings on Windows devices

11/1/2022 • 5 minutes to read • Edit Online

Use this article as guide to configure Microsoft Edge policy settings on Windows devices. If you haven't set up Microsoft Edge, see the Microsoft Edge setup guide.

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

Introduction to policy settings on Windows

You can use *group policy objects (GPO)* to configure policy settings for Microsoft Edge and managed Microsoft Edge updates on all versions of Windows. You can also configure policies via the registry for:

- Windows devices that are joined to a Microsoft Active Directory (AD) domain
- Windows 10 Pro or Enterprise instances enrolled for device management in Microsoft Intune

To configure Microsoft Edge with group policy objects, install *administrative templates* that add rules and settings for Microsoft Edge to the group policy Central Store in your Active Directory domain. Alternatively, add these rules and settings to the Policy Definition template folder on individual computers and then configure the specific policies you want to set.

You can use Active Directory group policy to configure Microsoft Edge policy settings if you prefer to manage policy at the domain level. This approach lets you manage policy settings globally. You can target different policy settings to specific OUs, or use WMI filters to apply settings only to users or computers returned by a particular query. To configure policies on individual computers, you can use Local Group Policy Editor on the target computer. This approach lets you apply policy settings that only affect the local device.

Microsoft Edge supports *mandatory* and *recommended* policies. Mandatory policies override user preferences and prevent the user from the policy. Recommended policies provide a default setting that the user can override. Most policies are only mandatory but there's a subset that is mandatory and recommended. If both versions of a policy are set, the mandatory setting takes precedence. A recommended policy only takes effect when the user hasn't modified the setting.

> **TIP**
> You can use Microsoft Intune to configure Microsoft Edge policy settings. For more information, see Configure Microsoft Edge using Microsoft Intune.

There are two administrative templates for Microsoft Edge, both can be applied with common group policy management tools such as Local Group Policy Editor for application on an individual computer or the Group Policy Management Console for Microsoft Windows domain networks. These templates are:

- *msedge.admx* to configure Microsoft Edge settings
- *msedgeupdate.admx* to manage Microsoft Edge updates

The following steps describe how to install, configure, and test the Microsoft Edge templates.

1. Download and install the Microsoft Edge administrative template

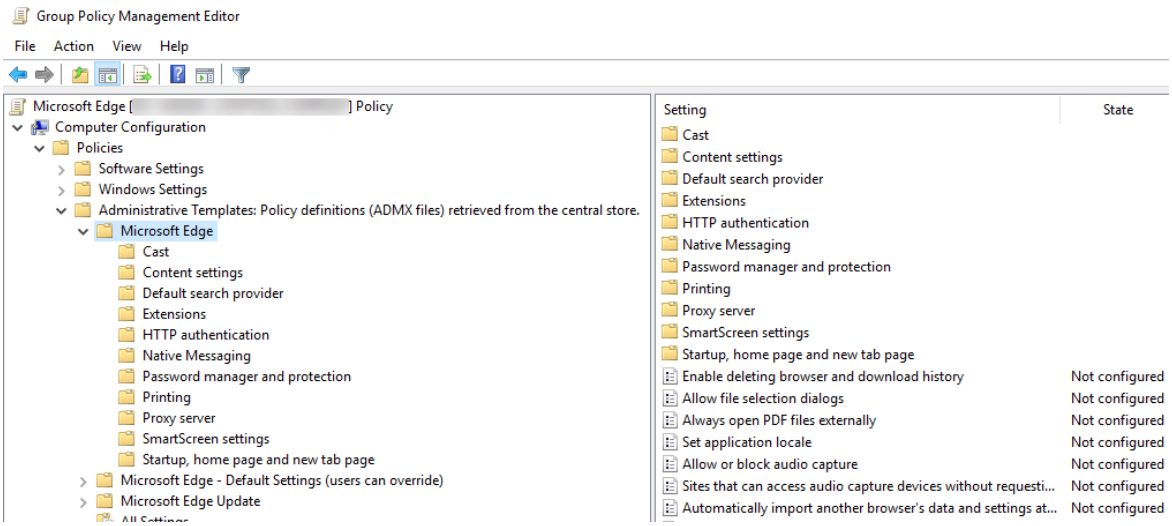
If you want to configure Microsoft Edge policy settings in Active Directory, download the files to a network location you can access from a domain controller or a workstation with the Remote Server Administration Tools (RSAT) installed. To configure on an individual computer,download the files to that computer.

When you add the administrative template files to the appropriate location, Microsoft Edge policy settings are immediately available in the Group Policy Editor.

Go to the Microsoft Edge Enterprise landing page to download the Microsoft Edge policy templates file and extract the contents.

Add the administrative template to Active Directory

1. On a domain controller or workstation with RSAT, go to the **PolicyDefinition** folder (also known as the *Central Store*) on any domain controller for your domain. For older versions of Windows Server, you might need to create the **PolicyDefinition** folder. For more information, see How to create and manage the Central Store for Group Policy Administrative Templates in Windows.
2. Open *MicrosoftEdgePolicyTemplates* and go to **windows** > **admx**.
3. Copy the *msedge.admx* file to the PolicyDefinition folder. (Example: %systemroot%\sysvol\domain\policies\PolicyDefinitions)
4. In the *admx* folder, open the appropriate language folder. For example, if you're in the U.S., open the **en-US** folder.
5. Copy the *msedge.adml* file to the matching language folder in the PolicyDefinition folder. Create the folder if it doesn't already exist. (Example: %systemroot%\sysvol\domain\policies\PolicyDefinitions\EN-US)
6. If your domain has more than one domain controller, the new ADMX files will be replicated to them at the next domain replication interval.
7. To confirm the files loaded correctly, open the **Group Policy Management Editor** from Windows Administrative Tools and expand **Computer Configuration** > **Policies** > **Administrative Templates** > **Microsoft Edge**. You should see one or more Microsoft Edge nodes as shown below.



Add the administrative template to an individual computer

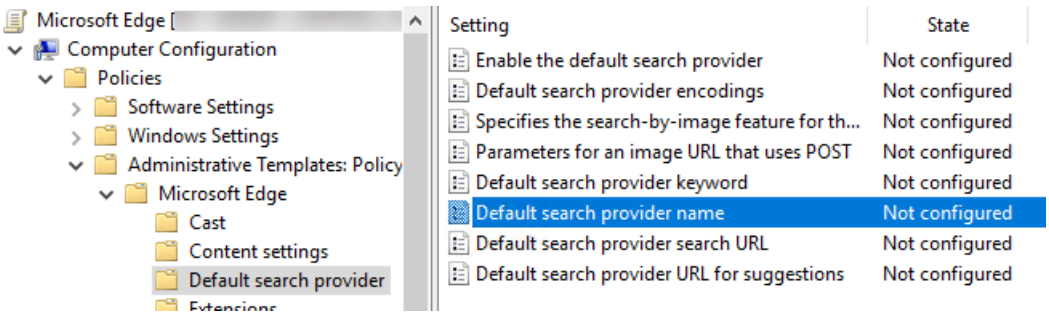
1. On the target computer, open *MicrosoftEdgePolicyTemplates* and go to **windows** > **admx**.
2. Copy the *msedge.admx* file to your Policy Definition template folder. (Example: C:\Windows\PolicyDefinitions)
3. In the *admx* folder, open the appropriate language folder. For example, if you're in the U.S., open the **en-US** folder.

4. Copy the *msedge.adml* file to the matching language folder in your Policy Definition folder. (Example: C:\Windows\PolicyDefinitions\en-US)
5. To confirm the files loaded correctly, open Local Group Policy Editor directly (Windows key + R and enter gpedit.msc) or open MMC and load the Local Group Policy Editor snap-in. If an error occurs, it's usually because the files are in an incorrect location.

2. Set mandatory or recommended policies

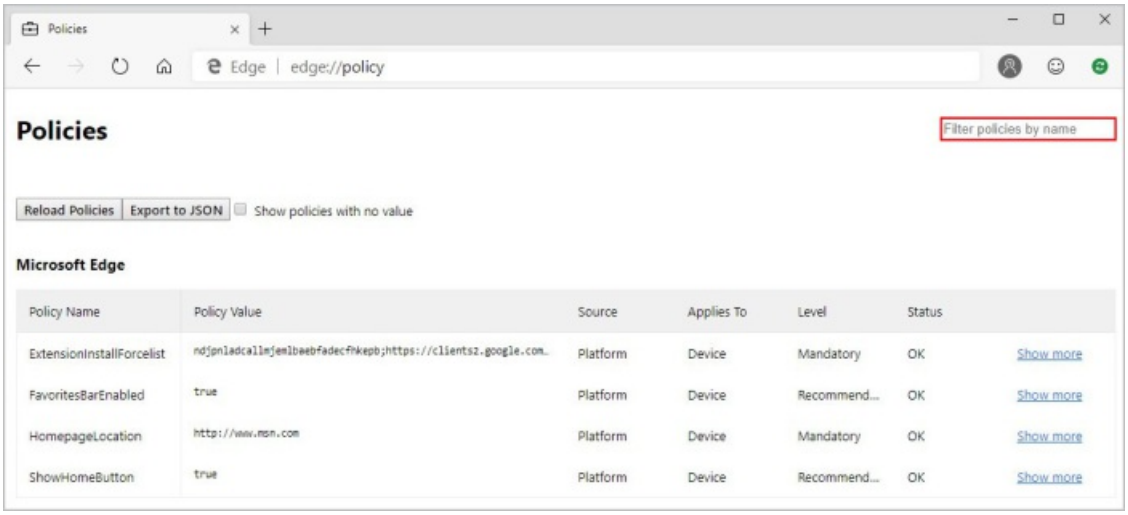
You can set mandatory or recommended policies to configure Microsoft Edge with the Group Policy Editor for both Active Directory and individual computers. You can scope policy settings to either the **Computer Configuration** or **User Configuration** by selecting the appropriate node as described below.

- To configure a mandatory policy, open the Group Policy Editor and go to (**Computer Configuration** or **User Configuration**) > **Policies** > **Administrative Templates** > **Microsoft Edge**.
- To configure a recommended policy, open the Group Policy Editor and go to (**Computer Configuration** or **User Configuration**) > **Policies** > **Administrative Templates** > **Microsoft Edge – Default Settings (users can override)**.



3. Test your policies

On a target client device, open Microsoft Edge and go to **edge://policy** to see all policies that are applied. If you applied policy settings on the local computer, policies should appear immediately. You might need to close and reopen Microsoft Edge if it was open while you were configuring policy settings.



For Active Directory group policy settings, policy settings are sent to domain computers at a regular interval defined by your domain administrator. Target computers might not receive policy updates right away. If you want to manually refresh Active Directory group policy settings on a target computer, run the following command from a command prompt or PowerShell session on the target computer:

```
gpupdate /force
```

You might need to close and reopen Microsoft Edge before the new policies appear.

You can also use REGEDIT.exe on a target computer to view the registry settings that store group policy settings. These policy settings are located at this registry path: **HKLM\SOFTWARE\Policies\Microsoft\Edge**.

See also

- Microsoft Edge Enterprise landing page
- Configure for Windows with Intune
- Configure for macOS
- Browse Microsoft Edge Enterprise Policies

Configure Microsoft Edge using Initial Preferences settings for the first run

11/1/2022 • 2 minutes to read • Edit Online

Use the information in this article to configure Microsoft Edge Initial Preferences settings on your Windows devices.

> **NOTE**
> This article applies to Microsoft Edge version 93 or later.

Configure policy settings on Windows

Starting Microsoft Edge release 93, Microsoft supports a limited number of Initial Preferences, formerly named "Master Preferences", to help admins configure browsers for the first run. For more information, see the supported settings in the following Preference settings table.

When deployed, Initial Preferences act as the default browser settings on managed devices. These preferences are the settings preferred by admins to be used as default browser settings for the first run.

> **NOTE**
> Initial preferences can be changed by users and aren't available for some devices because they aren't joined to an Active Directory® domain.

Some examples of initial preferences settings include initial configuration of a default homepage or tabs with specific URLs.

Preferences are only copied once from the *initial_preferences* file, changes made to this file after configuration won't be respected. If a setting is managed by a Microsoft Edge policy and configured in the *initial_preferences file*, the policy always takes precedence.

Preference settings

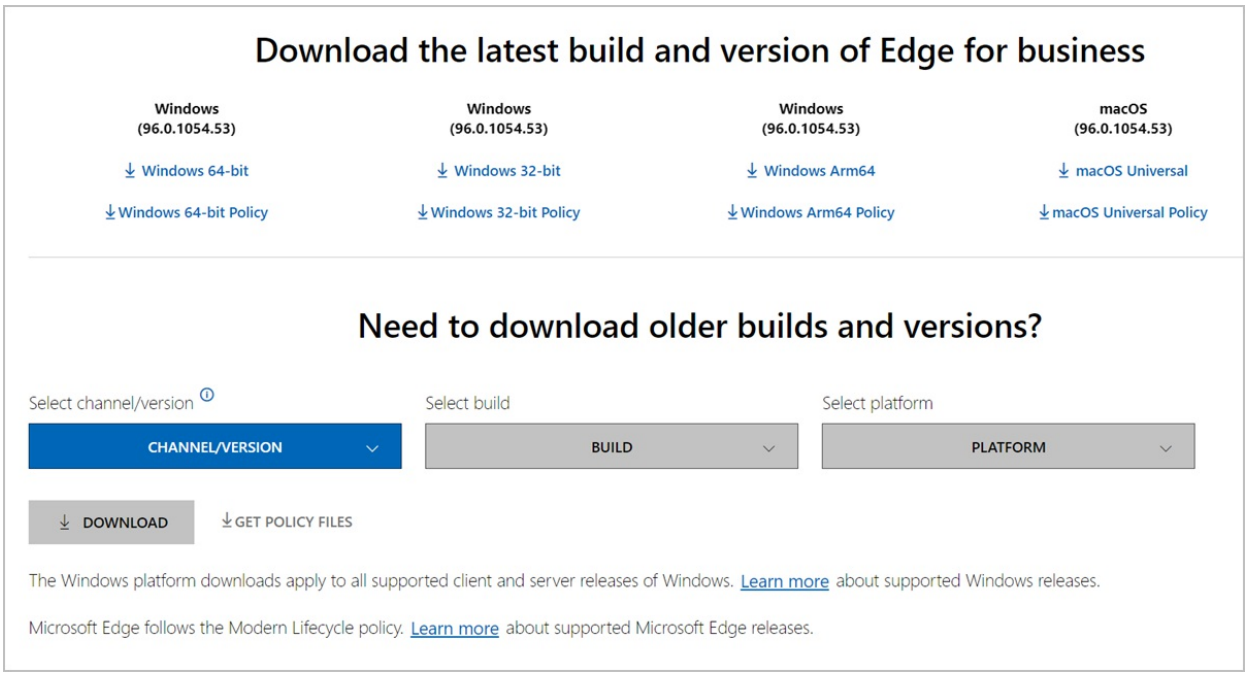
The following table shows the settings that are currently supported by Microsoft Edge.

PREFERENCES CATEGORY	SETTING
Bookmark_bar	show_apps_shortcut show_managed_bookmarks show_on_all_tabs
Bookmarks	editing_enabled

PREFERENCES CATEGORY	SETTING
Browser / clear_data	browsing_history browsing_history_basic" cache cache_basic cookies download_history form_data passwords
History	browsing_history cache cookies download_history form_data hosted_apps_data passwords site_settings
Browser	first_run_tabs dark_theme show_toolbar_bookmarks_button show_toolbar_collections_butto show_toolbar_downloads_button show_home_button show_prompt_before_closing_tabs show_toolbar_history_button
default_search_provider	[default_search_provider] enabled
Fullscreen	Allowed
homepage	Homepage_url
homepage_is_newtabpage	homepage_is_newtabpage
Session	restore_on_startup startup_urls
Extensions	Extensions: settings

1: Download an example initial_preferences file

To get started, download the "Policy" file from the Microsoft Edge Enterprise landing page. Extract the files in the download, and then open the *initial_preferences* file in the *examples* folder. The next screenshot shows the policy file options that are available to download



2: Customize and validate the initial_preferences file

Customize the preferences settings in the downloaded *initial_preferences* file and validate the changes to make sure that there are no errors in the JSON code. If you find errors, check the syntax and structure of the *initial_preferences* file, make corrections, and check it again. Few example tools to validate JSON, Online JSON Tools or JSON editing in Visual Studio Code.

3: Deploy preferences to users' computer

Deploy the *initial_preferences* file to users' devices at the same time as Microsoft Edge is deployed and put the file in the following location on the device.

Windows (AMD64 and ARM64)

CHANNEL	LOCATION
Stable	`"C:\Program Files (x86)\Microsoft\Edge\Application"`
Beta	`"C:\Program Files (x86)\Microsoft\Edge Beta\Application"`
Canary	`"%LOCALAPPDATA%\Microsoft\Edge SxS\Application"`
Dev	`"C:\Program Files (x86)\Microsoft\Edge Dev\Application"`

> **NOTE**
> The *initial_preferences* file needs to be deployed to the same folder as the *msedge.exe* file on users' Windows computers.

macOS

CHANNEL	LOCATION
Stable	`"~/Library/Application Support/Microsoft Edge/Microsoft Edge Initial Preferences"`

CHANNEL	LOCATION
Beta	`“~/Library/Application Support/Microsoft Edge Beta/Microsoft Edge Initial Preferences"`
Canary	`“~/Library/Application Support/Microsoft Edge Canary/Microsoft Edge Initial Preferences"`
Dev	`"~/Library/Application Support/Microsoft Edge Dev/Microsoft Edge Initial Preferences"`

Important notes: MSI / Pkg Deployment and *initial_preferences* interaction

Initial preferences will only take effect after the *initial_preferences* file is deployed before the browser's first run by the end users.

See also

- Policy download location

Per-site configuration by policy

11/1/2022 • 5 minutes to read • Edit Online

This article describes the per-site configurations by policy and how the browser handles page loads from a site.

The browser as a decision maker

As a part of every page load, browsers make many decisions. Some, but not all, of these decisions include: whether a particular API is available, should a resource load be permitted, and should a script be allowed to run.

In most cases, browser decisions are governed by the following inputs:

- A user setting
- The URL of the page for which the decision is made

In the Internet Explorer web platform, each of these decisions was called a URLAction. For more information, see URL Action Flags. The URLAction, Enterprise Group Policy, and user settings in the Internet Control Panel controlled how the browser would handle each decision.

In Microsoft Edge, most per-site permissions are controlled by settings and policies expressed using a simple syntax with limited wild-card support. Windows Security Zones are still used for a few configuration decisions.

Windows Security Zones

To simplify configuration for the user or admin, the legacy platform classified sites into one of fivedifferentSecurity Zones. These Security Zones are: Local Machine, Local Intranet, Trusted, Internet, and Restricted Sites.

When making a page load decision, the browser maps the website to a Zone, then consults the setting for the URLAction for that Zone to decide what to do. Reasonable defaults like "Automatically satisfy authentication challenges from my Intranet" means that most users never need to change any default settings.

Users can use the Internet Control Panel to assign specific sites to Zones and to configure the permission results for each zone. In managed environments, administrators can use Group Policy to assign specific sites to Zones (via "Site to Zone Assignment List" policy) and specify the settings for URLActions on a per-zone basis. Beyond manual administrative or user assignment of sites to Zones, other heuristics couldassign sites to the Local Intranet Zone. In particular, dotless host names (for example, `http://payroll`) were assigned to the Intranet Zone. If aProxy Configuration scriptwas used, any sites configured to bypass the proxy would be mapped to the Intranet Zone.

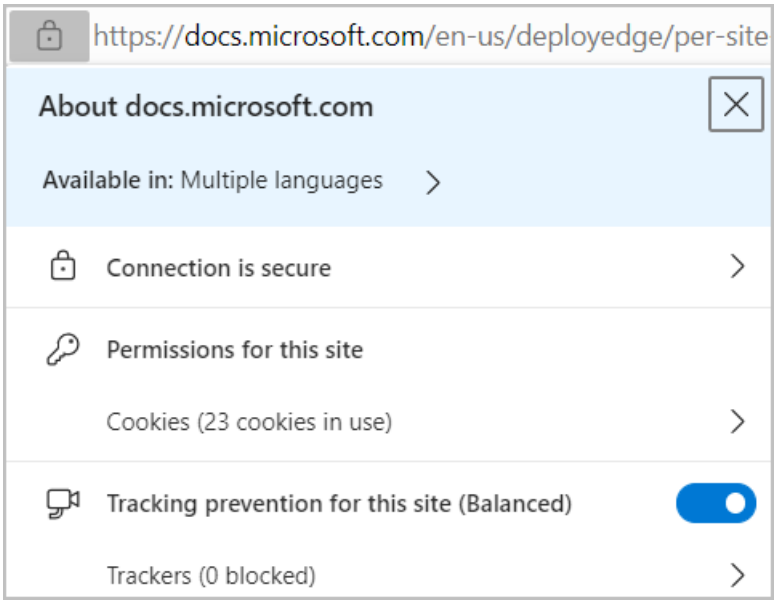
Microsoft Edge Legacy inherited the Zones architecture from its Internet Explorer predecessor with a few simplifying changes:

- Windows' five built-in Zones were collapsed to three: Internet (Internet), Trusted (Intranet+Trusted), and Local Computer. The Restricted Sites Zone was removed.
- Zone to URLAction mappings were hardcoded into the browser, ignoring Group Policies and settings in the Internet Control Panel.

Per site permissions in Microsoft Edge

Microsoft Edge makeslimited useof Windows Security Zones. Instead, mostpermissions and featuresthat offer administrators per-site configuration viapolicy rely on lists of rules in theURL Filter Format.

When end users opena settings page like `edge://settings/content/siteDetails?site=https://example.com`, they'll find a long list of configuration switches and lists for various permissions. Users rarely use the Settings page directly, instead they make choices while browsing and using various widgets and toggles in the**page info**dropdown. This list appears when you select the lock icon in the address bar. You can also use the various prompts or buttons at the right-edge of the address bar. The next screenshot shows an example of page information.



Enterprises can useGroup Policy to set up site lists for individual policies that control the browser's behavior. To find these policies, open theMicrosoft Edge Group Policy documentationand search for"ForUrls"to find the policies that allow and block behavior based on the loaded site's URL. Most of the relevant settings are listed in theGroup Policy for Content Settings section.

There are also many policies (whose names contain"Default") that control the default behavior for a given setting.

Many of the settings are obscure (WebSerial, WebMIDI) and there's often no reason to change a setting from the default.

Security Zones inMicrosoft Edge

While Microsoft Edge relies mostly on individual policies using the URL Filter format, it continues to use Windows' Security Zones by default in a few cases. This approach simplifies deployment in Enterprises that have historically relied upon Zones configuration.

The following behaviors are controlled by Zone policy:

- Decidingwhether to release Windows Integrated Authentication (Kerberos or NTLM) credentials automatically.
- Decidinghow to handle file downloads.
- For Internet Explorer mode.

Credential release

By default, Microsoft Edge evaluates `URLACTION_CREDENTIALS_USE` to decide whether Windows Integrated Authentication is used automatically, or if the user will see a manual authentication prompt. Configuring the AuthServerAllowlist site list policy will prevent Zone Policy from being consulted.

File downloads

Evidence about the origins of a file download (also known as "Mark of the Web" is recorded for files downloaded from the Internet Zone. Other applications, such as the Windows Shell, and Microsoft Office may take this origin evidence into account when deciding how to handle a file.

If the Windows Security Zone policy is configured to disablethe settingfor launching applications and download unsafe files, Microsoft Edge's download manager will block file downloads from sites in that Zone. A user will see this note: "Couldn't download – Blocked".

IE mode

IE mode can be configured toopen all Intranet sites in IE mode. When using this configuration, Microsoft Edge evaluates the Zone of a URL when deciding whether or not it should open in IE mode. Beyond this initial decision, IE mode tabs arereallyrunning Internet Explorer, and as a result they evaluate Zones settings for every policy decision just as Internet Explorer did.

Summary

In most cases, Microsoft Edge settings can be left at their defaults. Administrators who wish to change the defaults for all sites or specific sites can use the appropriate Group Policies to specify Site Lists or default behaviors. In a handful of cases, such as credential release, file download, and IE mode, admins will continue to control behavior by configuring Windows Security Zones settings.

Frequently asked questions

Can the URL filter format match on a site's IP address?

No, the format doesn't support specifying an IP range for allowlists and blocklists. It does support specification of individual IP**literals**, but such rules are only respected if the user navigates to the site using said literal (for example, `http://127.0.0.1/`). If a hostname is used (`http://localhost`), the IP Literal rule will not be respected even though the resolved IP of the host matches the filter-listed IP.

Can URL filters matchdotless host names?

No. You must list each hostname, for example `https://payroll`, `https://stock`, `https://who`, and so on.

If you were forward-thinking enough to structure your intranet such that your host names are of the following form, then you've implemented a best practice.

- `https://payroll.contoso-intranet.com`
- `https://timecard.contoso-intranet.com`
- `https://sharepoint.contoso-intranet.com`

In the preceding scenario, you can configure each policy with a*.**contoso-intranet.com**entry and your entire intranet will be opted in.

See also

- Microsoft Edge documentation
- Microsoft Edge Enterprise landing page

Configure Microsoft Edge using Mobile Device Management

11/1/2022 • 11 minutes to read • Edit Online

This article explains how to configure Microsoft Edge on Windows 10 using Mobile Device Management (MDM) with ADMX Ingestion. This article also describes:

- How to create Open Mobile Alliance Uniform Resource Identifier (OMA-URI) for Microsoft Edge policies.
- How to configure Microsoft Edge in Intune using ADMX ingestion and custom OMA-URI.

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

Prerequisites

Windows 10, with the following minimum system requirements:

- Windows 10, version 1903 with KB4512941 and KB4517211 installed
- Windows 10, version 1809 with KB4512534 and KB4520062 installed
- Windows 10, version 1803 with KB4512509 and KB4519978 installed
- Windows 10, version 1709 with KB4516071 and KB4520006 installed

Overview

You can configure Microsoft Edge on Windows 10 using MDM with your preferred Enterprise Mobility Management (EMM) or MDM provider that supports ADMX Ingestion.

Configuring Microsoft Edge with MDM is a two part process:

1. Ingesting the Microsoft Edge ADMX file into your EMM or MDM provider. See your provider for instructions on how to ingest an ADMX file.

   > **NOTE**
   > For Microsoft Intune, see Configure Microsoft Edge in Intune using ADMX ingestion.

2. Creating an OMA-URI for a Microsoft Edge policy.

Create an OMA-URI for Microsoft Edge policies

The following sections describe how to create the OMA-URI path and look up and define the value in XML format for mandatory and recommended browser policies.

Before you get started, download the Microsoft Edge policy templates file (MicrosoftEdgePolicyTemplates.cab) from the Microsoft Edge Enterprise landing page and extract the contents.

There are three steps for defining the OMA-URI:

1. Create the OMA-URI path
2. Specify the OMA-URI data type
3. Set the OMA-URI value

Create the OMA-URI path

Use the following formula as a guide for creating the OMA-URI paths.

```
./Device/Vendor/MSFT/Policy/Config/<ADMXIngestName>~Policy~<ADMXNamespace>~<ADMXCategory>/<PolicyName>
```

PARAMETER	DESCRIPTION
<ADMXIngestName>	Use "Edge" or what you defined when ingesting the administrative template. For example, if you used "./Device/Vendor/MSFT/Policy/ConfigOperations/ADMXInstall/MicrosoftEdge/Policy/EdgeAdmx", then use "MicrosoftEdge". The `<ADMXIngestionName>` must match what was used when you ingested the ADMX file.
<ADMXNamespace>	Either "microsoft_edge" or "microsoft_edge_recommended" depending on whether you're setting a mandatory or recommended policy.
<ADMXCategory>	The "parentCategory" of the policy is defined in the ADMX file. Omit the `<ADMXCategory>` if the policy isn't grouped (No "parentCategory" defined).
<PolicyName>	The policy name can be found in the Browser policy reference article.

URI path example:

For this example, assume the `<ADMXIngestName>` node was named "Edge" and you're setting a mandatory policy. The URI path would be:

`./Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge~<ADMXCategory>/<PolicyName>`

If the policy isn't in a group (for example, DiskCacheSize) remove "`~<ADMXCategory>`". Replace `<PolicyName>` with the name of the policy, DiskCacheSize. The URI path would be:

`./Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge/DiskCacheSize`

If the policy is in a group, follow these steps:

1. Open **msedge.admx** with any xml editor.
2. Search for the policy name you want to set. For example, "ExtensionInstallForceList".
3. Use the value of the *ref* attribute from the *parentCategory* element. For example, "Extensions" from <parentCategory ref=" Extensions"/>.
4. Replace `<ADMXCategory>` with the *ref* attribute value to construct the URI path. The URI path would be:

`/Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge~Extensions/ExtensionInstallForcelist`

Specify the data type

The OMA-URI data type is always "String".

Set the value for a browser policy

This section describes how to set the value, in XML format, for each data type. Go to Browser policy reference to look up the data type of the policy.

> **NOTE**
> For non-Boolean data types, the value always starts with `<enabled/>`.

Boolean data type

For policies that are Boolean types use `<enabled/>` or `<disabled/>`.

Integer data type

The value always needs to start with the `<enabled/>` element followed by `<data id="[valueName]" value="[decimal value]"/>`.

To find the value name and decimal value for a new tab page, use the following steps:

1. Open **msedge.admx** with any xml editor.
2. Search for the `<policy>` element where the name attribute matches the policy name you want to set. For "RestoreOnStartup", search for `name="RestoreOnStartup"`.
3. In the `<elements>` node, find the value you want to set.
4. Use the value in the "valueName" attribute in the `<elements>` node. For "RestoreOnStartup" the "valueName" is "RestoreOnStartup".
5. Use the value in the "value" attribute in the `<decimal>` node. For "RestoreOnStartup" to open the new tab page the value is "5".

To open the new tab page on startup use:
`<enabled/> <data id="RestoreOnStartup" value="5"/>`

List of strings data type

The value always needs to start with the `<enabled/>` element followed by `<data id="[listID]" value="[string 1];[string 2];[string 3]"/>`.

> **NOTE**
> The "id=" attribute name isn't the policy name, even though in most cases it matches the policy name. It's the <list> node id attribute value, which is found in the ADMX file.

To find the listID and define the value to block a URL, follow these steps:

1. Open **msedge.admx** with any xml editor.
2. Search for the `<policy>` element where the name attribute matches the policy name you want to set. For "URLBlocklist", search for `name="URLBlocklist"`.
3. Use the value in the "id" attribute of the `<list> node for [listID]`.
4. The "value" is a list of URLs separated by a semicolon (;)

For example, to block access to `contoso.com` and `https://ssl.server.com`:
`<enabled/> <data id=" URLBlocklistDesc" value="contoso.com;https://ssl.server.com"/>`

Dictionary or String data type

The value always needs to start with the `<enabled/>` followed by `<data id="[textID]" value="[string]"/>`.

To find the textID and define the value set the locale, follow these steps:

1. Open **msedge.admx** with any xml editor.
2. Search for the `<policy>` element where the name attribute matches the policy name you want to set. For "ApplicationLocaleValue", search for `name="ApplicationLocaleValue"`.
3. Use the value in the "id" attribute of the `<text>` node for `[textID]`.
4. Set the "value" to the culture code.

To set the locale to "es-US" with the "ApplicationLocaleValue" policy:
`<enabled/> <data id="ApplicationLocaleValue" value="es-US"/>`

Dictionary data types are treated as large strings but normally need string escaping to get the value into the correct form.

For example, to set the ManagedFavorites policy the value would be:

```
<enabled/> <data id="ManagedFavorites" value="[{&quot;toplevel_name&quot;: &quot;My managed favorites
folder&quot;}, {&quot;name&quot;: &quot;Microsoft&quot;, &quot;url&quot;: &quot;microsoft.com&quot;},
{&quot;name&quot;: &quot;Bing&quot;, &quot;url&quot;: &quot;bing.com&quot;}, {&quot;children&quot;:
[{&quot;name&quot;: &quot;Microsoft Edge Insiders&quot;, &quot;url&quot;:
&quot;www.microsoftedgeinsider.com&quot;}, {&quot;name&quot;: &quot;Microsoft Edge&quot;, &quot;url&quot;:
&quot;www.microsoft.com/windows/microsoft-edge&quot;}], &quot;name&quot;: &quot;Microsoft Edge
links&quot;}]"/>
```

Create the OMA-URI for recommended policies

Defining the URI path for recommended policies depends on the policy you want to configure.

To define the URI path for a recommended policy

Use the URI path formula (`./Device/Vendor/MSFT/Policy/Config/<ADMXIngestName>~Policy~<ADMXNamespace>~<ADMXCategory>/<PolicyName>`) and the following steps to define the URI path:

1. Open **msedge.admx** with any xml editor.
2. If the policy you want to configure isn't in a group, skip to step 4 and remove `~<ADMXCategory>` from the path.
3. If the policy you want to configure is in a group:
   - To look up the `<ADMXCategory>`, search for the policy you want to set. When searching append "_recommended" to the policy name. For example, a search for "RegisteredProtocolHandlers_recommended" has the following result:

     ```
     <policy class="Both" displayName="$(string.RegisteredProtocolHandlers)"
     explainText="$(string.RegisteredProtocolHandlers_Explain)"
     key="Software\Policies\Microsoft\Edge\Recommended"
     name="RegisteredProtocolHandlers_recommended"
     presentation="$(presentation.RegisteredProtocolHandlers)">
        <parentCategory ref="ContentSettings_recommended"/>
        <supportedOn ref="SUPPORTED_WIN7_V77"/>
        <elements>
          <text id="RegisteredProtocolHandlers" maxLength="1000000"
     valueName="RegisteredProtocolHandlers"/>
        </elements>
     </policy>
     ```

   - Copy the value of the *ref* attribute from the `<parentCategory>` element. For "ContentSettings", copy "ContentSettings_recommended" from `<parentCategory ref=" ContentSettings_recommended"/>`.
   - Replace `<ADMXCategory>` with the *ref* attribute value to construct the URI path in the URI path formula.
4. The `<PolicyName>` is the name of the policy with "_recommended" appended to it.

OMA-URI path examples for recommended policies

The following table shows examples of OMA-URI paths for recommended policies.

POLICY	OMA-URI
RegisteredProtocolHandlers	`./Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge_recommended~ContentSettings_recommende`
PasswordManagerEnabled	`./Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge_recommended~PasswordManager_recommende`
PrintHeaderFooter	`./Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge_recommended~Printing_recommended/Print`
SmartScreenEnabled	`./Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge_recommended~SmartScreen_recommended/Sm`
HomePageLocation	`./Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge_recommended~Startup_recommended/Homepa`
ShowHomeButton	`./Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge_recommended~Startup_recommended/ShowHo`
FavoritesBarEnabled	`./Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge_recommended~/FavoritesBarEnabled_recom`

OMA-URI examples

OMA-URI examples with their URI path, type, and an example value.

Boolean data type examples

ShowHomeButton:

FIELD	VALUE
Name	Microsoft Edge: ShowHomeButton
OMA-URI	`./Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge~Startup/ShowHomeButton`
Type	String
Value	`<enabled/>`

DefaultSearchProviderEnabled:

FIELD	VALUE
Name	Microsoft Edge: DefaultSearchProviderEnabled

FIELD	VALUE
OMA-URI	`./Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge~DefaultSearchProvider/DefaultSearchPro`
Type	String
Value	`<disable/>`

Integer data type examples

AutoImportAtFirstRun:

FIELD	VALUE
Name	Microsoft Edge: AutoImportAtFirstRun
OMA-URI	`./Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge/AutoImportAtFirstRun`
Type	String
Value	`<enabled/><data id="AutoImportAtFirstRun" value="1"/>`

DefaultImagesSetting:

FIELD	VALUE
Name	Microsoft Edge: DefaultImagesSetting
OMA-URI	`./Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge~ContentSettings/DefaultImagesSetting`
Type	String
Value	`<enabled/><data id="DefaultImagesSetting" value="2"/>`

DiskCacheSize:

FIELD	VALUE
Name	Microsoft Edge: DiskCacheSize
OMA-URI	`./Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge/DiskCacheSize`
Type	String
Value	`<enabled/><data id="DiskCacheSize" value="1000000"/>`

List of strings data type examples

RestoreOnStartupURLS:

FIELD	VALUE
Name	Microsoft Edge: RestoreOnStartupURLS
OMA-URI	`./Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge~Startup/RestoreOnStartupURLs`
Type	String

Value	`<enabled/><data id="RestoreOnStartupURLsDesc" value="1http://www.bing.com"/>`
	For multiple list items:
	`<enabled/><data id="RestoreOnStartupURLsDesc" value="1http://www.bing.com2http://www.microsoft.com"/>`

ExtensionInstallForcelist:

FIELD	VALUE
Name	Microsoft Edge: ExtensionInstallForcelist
OMA-URI	`./Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge~Extensions/ExtensionInstallForcelist`
Type	String
Value	`<enabled/><data id="ExtensionInstallForcelistDesc" value="1gbchcmhmhahfdphkhkmpfmihenigjmpp;https://extensionwebstorebase.edgesv.net/v1/crx"/>`

Dictionary and String data type examples

ProxyMode:

FIELD	VALUE
Name	Microsoft Edge: ProxyMode
OMA-URI	`./Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge~ProxyMode/ProxyMode`

FIELD	VALUE
Type	String
Value	`<enabled/><data id="ProxyMode" value="auto_detect"/>`

ManagedFavorites:

FIELD	VALUE
Name	Microsoft Edge: ManagedFavorites
OMA-URI	`./Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge/ManagedFavorites`
Type	String
Value	`<enabled/> <data id="ManagedFavorites" value="[{"toplevel_name": "My managed favorites folder"}, {"name": "Microsoft", "url": "microsoft.com"}, {"name": "Bing", "url": "bing.com"}, {"children": [{"name": "Microsoft Edge Insiders", "url": "www.microsoftedgeinsider.com"}, {"name": "Microsoft Edge", "url": "www.microsoft.com/windows/microsoft-edge"}], "name": "Microsoft Edge links"}]"/>`

Configure Microsoft Edge in Intune using ADMX ingestion

The recommended way to configure Microsoft Edge with Microsoft Intune is to use the Administrative Templates profile. This profile is described in Configure Microsoft Edge policy settings with Microsoft Intune. If you want to evaluate a policy that's currently not available in the Microsoft Edge Administrative Templates in Intune, you can configure Microsoft Edge using custom settings for Windows 10 devices in Intune.

This section describes how to:

1. Ingest the Microsoft Edge ADMX file into Intune
2. Set a policy using custom OMA-URI in Intune

> **IMPORTANT**
> As a best practice, don't use a custom OMA-URI profile and an Administration templates profile to configure the same Microsoft Edge setting in Intune. If you deploy the same policy using both a custom OMA-URI and an Administrative template profile, but with different values, users will get unpredictable results. We strongly recommend removing your OMA-URI profile before using an Administration templates profile.

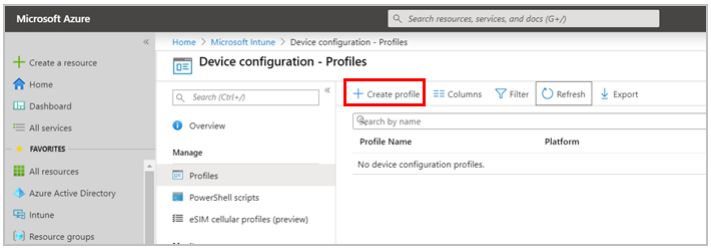
Ingest the Microsoft Edge ADMX file into Intune

This section describes how to ingest the Microsoft Edge administrative template (**msedge.admx** file) into Intune.

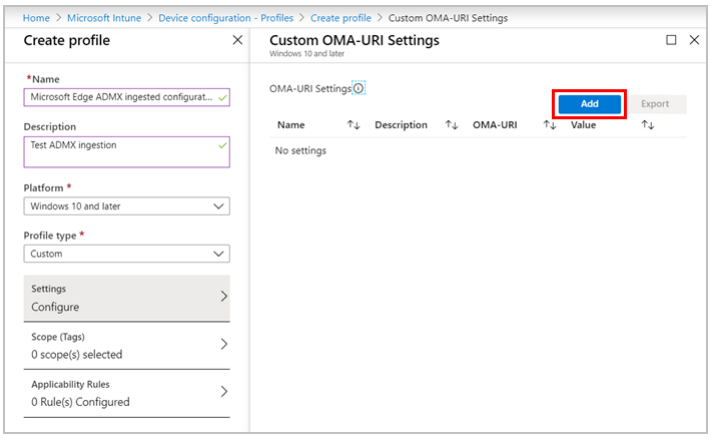
> **WARNING**
> Don't modify the ADMX file before ingesting the file.

To ingest the ADMX file, follow these steps:

1. Download the Microsoft Edge policy templates file (MicrosoftEdgePolicyTemplates.cab) from the Microsoft Edge Enterprise landing page and extract the contents. The file that you want to ingest is **msedge.admx**.
2. Sign in to the Microsoft Azure portal.
3. Select **Intune** from *All Services*, or search for Intune in the portal search box.
4. From *Microsoft Intune - Overview*, select **Device configuration** | **Profiles**.
5. On the top command bar, select **+ Create profile**.

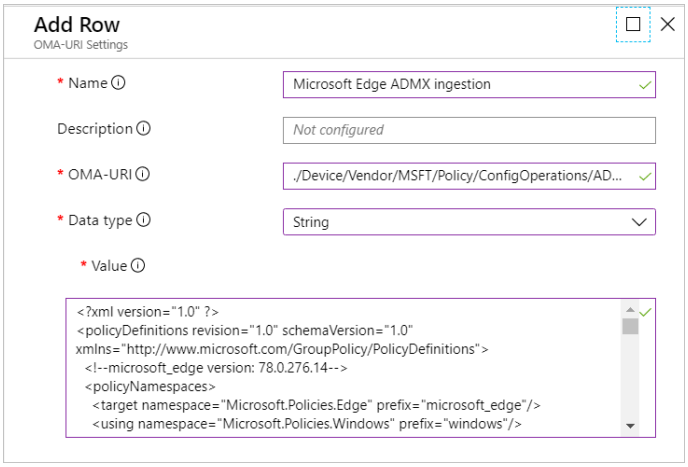


6. Provide the following profile information:
   - **Name**: Enter a descriptive name. For this example, "Microsoft Edge ADMX ingested configuration".
   - **Description**: Enter an optional description for the profile.
   - **Platform**: Select "Windows 10 and later"
   - **Profile type**: Select "Custom"
7. On **Custom OMA-URI Settings**, click **Add** to add an ADMX ingestion.



8. On **Add Row**, provide the following information:

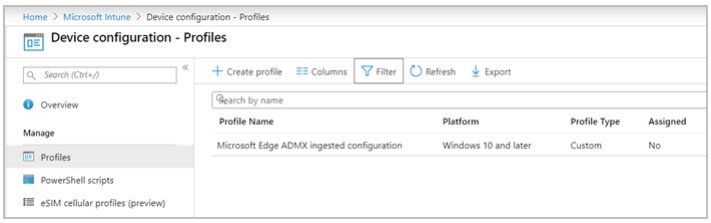
   - **Name**: Enter a descriptive name. For this example, use "Microsoft Edge ADMX ingestion".
   - **Description**: Enter an optional description for the setting.
   - **OMA-URI**: Enter "*./Device/Vendor/MSFT/Policy/ConfigOperations/ADMXInstall/Edge/Policy/EdgeAdmx*"
   - **Data type**: Select "String"
   - **Value**: This input area appears after you select the **Data type**. Open the msedge.admx file from the Microsoft Edge policy templates file you extracted in step 1. Copy **ALL the text** from the msedge.admx file and paste it in the **Value** text area shown in the following screenshot.



   - Click **OK**.

9. On **Custom OMA-URI Settings**, click **OK**.

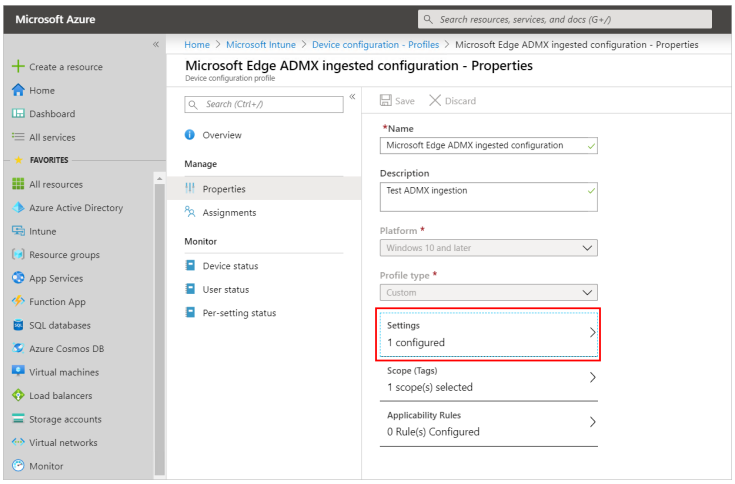
10. On **Create profile**, click **Create**. The next screenshot shows information about the newly created profile.



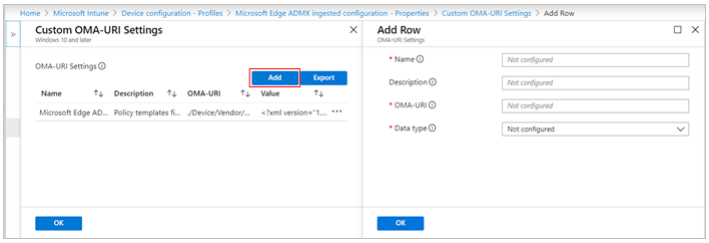
Set a policy using custom OMA-URI in Intune

> **NOTE**
> Before using the steps in this section you must complete the steps described in Ingest the Microsoft Edge ADMX file into Intune.

1. Sign in to the Microsoft Azure portal.
2. Select **Intune** from *All Services*, or search for Intune in the portal search box.
3. Go to **Intune**>**Device configuration**>**Profiles**.
4. Select the "Microsoft Edge ADMX ingested configuration" profile or the name you used for the profile.
5. To add Microsoft Edge policy settings, you have to open **Custom OMA-URI Settings**. Under **Manage**, click **Properties**, and then click **Settings**.

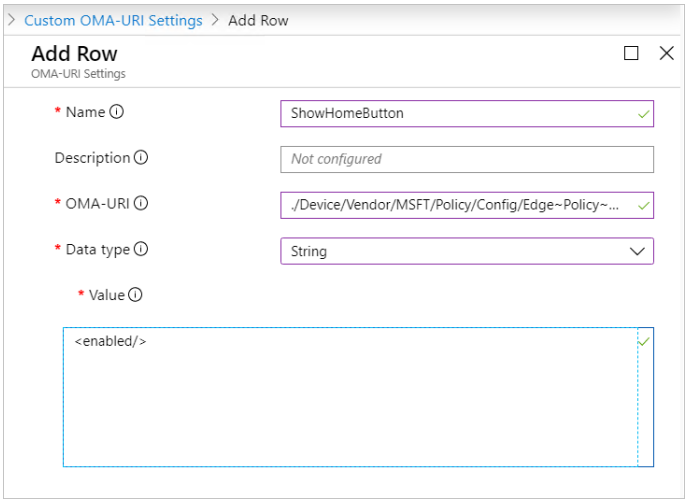


6. On **Custom OMA-URI Settings**, click **Add**.



7. On **Add Row**, provide the following information:

   - **Name**: Enter a descriptive name. We suggest using the policy name you want to configure. For this example, use "ShowHomeButton".
   - **Description** (Optional): Enter a description for the setting.
   - **OMA-URI**: Enter the OMA-URI for the policy. Using the for "ShowHomeButton" policy as an example, use this string: "*./Device/Vendor/MSFT/Policy/Config/Edge~Policy~microsoft_edge~Startup/ShowHomeButton*"
   - **Data type**: Select the policy settings data type. For the "ShowHomeButton" policy, use "String"
   - **Value**: Enter the setting that you want to configure for the policy. For "ShowHomeButton" example, enter "<enabled/>". The following screenshot shows the settings for configuring a policy.



   - Click **OK**.

8. On **Custom OMA-URI Settings**, click **OK**.
9. On the "**Microsoft Edge ADMX ingested configuration - Properties**" profile (or the name you used), click **Save**.

After the profile is created and the properties set, you have to assign the profile in Microsoft Intune.

Confirm that the policy was set

Use the following steps to confirm that the Microsoft Edge policy is using the profile you created. (Give Microsoft Intune time to propagate the policy to a device you assigned in the "Microsoft Edge ADMX ingested configuration" profile example.)

1. Open Microsoft Edge and go to *edge://policy*.
2. On the **Policies** page, see if the policy you set in the profile is listed.
3. If your policy isn't shown, see Diagnose MDM failures in Windows 10 or Troubleshoot a policy setting.

Troubleshoot a policy setting

If a Microsoft Edge policy isn't taking effect, try the following steps:

Open the *edge://policy* page on the target device (a device you assigned the profile to in Microsoft Intune) and search for the policy. If the policy isn't on the *edge://policy* page, try the following:

- Check that the policy is in the registry and is correct. On the target device open the Windows 10 Registry Editor (**Windows key + r**, enter "*regedit*" and then press **Enter**.) Check that the policy is correctly defined in the *\Software\Policies\ Microsoft\Edge* path. If you don't find the policy in the expected path, then the policy wasn't pushed to the device correctly.
- Check that the OMA-URI path is correct, and the value is a valid XML string. If either of these are incorrect the policy won't be pushed to the target device.

For more trouble shooting tips, see Set up Microsoft Intune and Sync devices.

See also

- Microsoft Edge Enterprise landing page
- Configure Microsoft Edge policy settings with Microsoft Intune
- Mobile device management
- Use custom settings for Windows 10 devices in Intune
- Win32 and Desktop Bridge app policy configuration
- Understanding ADMX-backed policies

Configure Microsoft Edge policy settings for macOS using a property list

11/1/2022 • 2 minutes to read • Edit Online

This article describes how to configure Microsoft Edge on macOS using a property list (.plist) file. You'll learn how to create this file and then deploy it to Microsoft Intune.

For more information, see About Information Property List Files (Apple's website) and Custom payload settings.

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

Configure Microsoft Edge policies on macOS

The first step is to create your plist. You can create the plist file with any text editor. Another option is to use Terminal to create the configuration profile. However, it's easier to create and edit a plist file with a tool that formats the XML code for you. *Xcode* is a free integrated development environment that's available at the following locations:

- Apple developer website
- Mac App Store

For a list of supported policies and their preference key names, see Microsoft Edge browser policies reference. In the policy templates file, which can be downloaded from the Microsoft Edge Enterprise landing page, there's a plist example (*itadminexample.plist*) in the **examples** folder. This file contains all supported data types that you can customize to define your policy settings.

After you create the contents of your plist, name the plist using the Microsoft Edge preference domain, which is "*com.microsoft.Edge*". This name is case-sensitive and shouldn't include the channel you're targeting because it applies to all Microsoft Edge channels. The plist file name must be ***com.microsoft.Edge.plist***.

> **IMPORTANT**
> Starting with build 78.0.249.2, all Microsoft Edge channels on macOS read from the **com.microsoft.Edge** preference domain. All prior releases read from a channel specific domain, such as **com.microsoft.Edge.Dev** for Dev channel.

The last step is to deploy your plist to your users' Mac devices using your preferred MDM provider, such as Microsoft Intune. For instructions see Deploy your plist.

Create a configuration profile using Terminal

1. In Terminal, use the following command to create a plist for Microsoft Edge on your desktop with your preferred settings:

   ```
   /usr/bin/defaults write ~/Desktop/com.microsoft.Edge.plist RestoreOnStartup -int 1
   ```

2. Convert the plist from binary to plain text format:

```
/usr/bin/plutil -convert xml1 ~/Desktop/com.microsoft.Edge.plist
```

After converting the file verify that your policy data is correct and contains the settings, you want for your configuration profile.

> **NOTE**
>
> Only key value pairs should be in the contents of the plist or xml file. Prior to uploading your file into Intune remove all the <plist> and <dict> values, and xml headers from your file. The file should only contain key value pairs.

Deploy your plist

Using Microsoft Intune, create a new device configuration profile targeting the macOS platform and select the *Preference file* profile type. Target **com.microsoft.Edge** as the preference domain name and upload your plist. For more information, see Add a property list file to macOS devices using Microsoft Intune.

For Jamf, upload the .plist file as a *Custom Settings* payload.

See also

- Microsoft Edge Enterprise landing page
- Configure for macOS with Jamf
- Configure for Windows
- Configure for Windows with Intune

Configure Microsoft Edge policy settings on macOS with Jamf

11/1/2022 • 3 minutes to read • Edit Online

This article describes how to configure policy settings on macOS using a Microsoft Edge policy manifest file on Jamf Pro 10.19.

You can also configure Microsoft Edge policy settings on macOS by using a property list (.plist) file. For more information, see Configure for macOS using a .plist

Prerequisites

The following software is required:

- Microsoft Edge Stable channel 81
- Policy Templates file, version 81.0.416.3
- Jamf Pro, Version 10.19

About the Jamf Pro Application & Custom Settings menu

Before Jamf Pro 10.18, managing Office 365 involved manually building a .plist file. This was a time-consuming workflow that required a strong technical background. Jamf Pro 10.18 eliminated those barriers by streamlining the configuration process. However, IT Admins could only use this new user interface for specific applications and preference domains specified by Jamf.

In Jamf Pro 10.19, a user can upload a JSON manifest as a "custom schema" to target any preference domain, and the graphical user interface will be generated from this manifest. The custom schema that's created follows the JSON Schema specification.

For more information, see Computer Configuration Profiles in the Jamf Pro Administrator's Guide.

Get the policy manifest for a specific version of Microsoft Edge

To get the policy manifest:

- Go to the Microsoft Edge Enterprise landing page.
- On the Channel/Version dropdown list, select **any channel with version 81 or later.***.
- On the Build dropdown list, select any **81 build or later.***.
- Click GET POLICY FILES to download our policy templates bundle.

> **NOTE**
> Currently, the policy templates bundle is signed as a CAB file. You'll need to use a 3rd party tool, such as The Unarchiver to open the file on macOS.

After you unpack the CAB file, unpack the ZIP file and navigate to the "mac" top level directory. The manifest, which is named "policy_manifest.json", is in this directory.

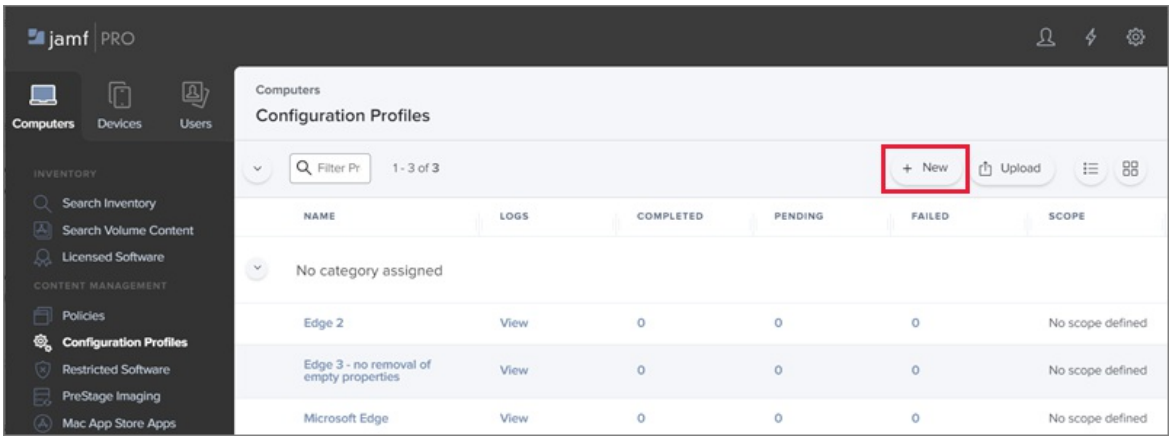
This manifest will be published in every policy bundle starting with build 81.0.416.3. If you want to test policies

in the Dev channel, you can take the manifest associated with each Dev release and test it in Jamf Pro.

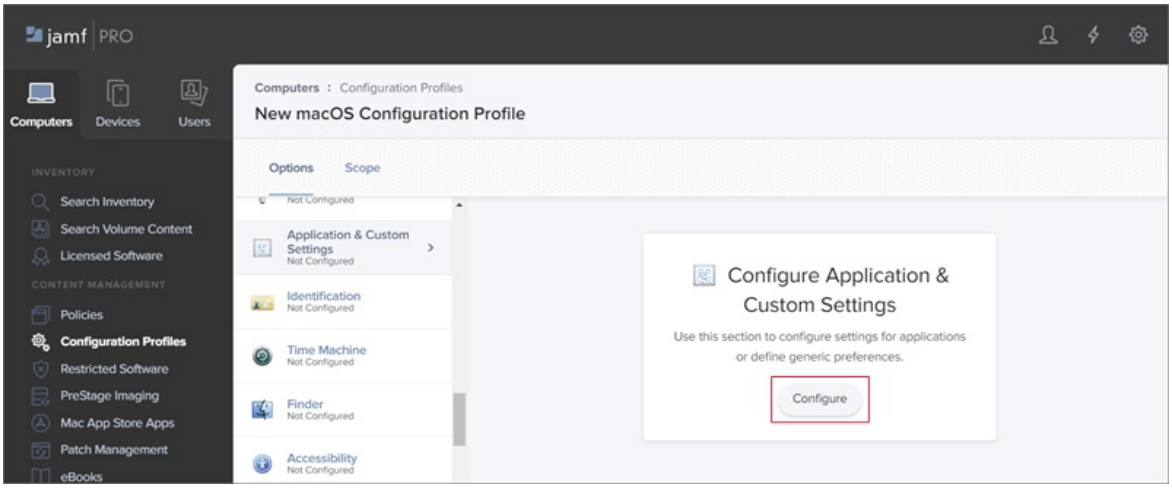
Use the policy manifest in Jamf Pro

Use the following steps to upload the policy manifest to Jamf Pro and then create a policy profile for macOS.

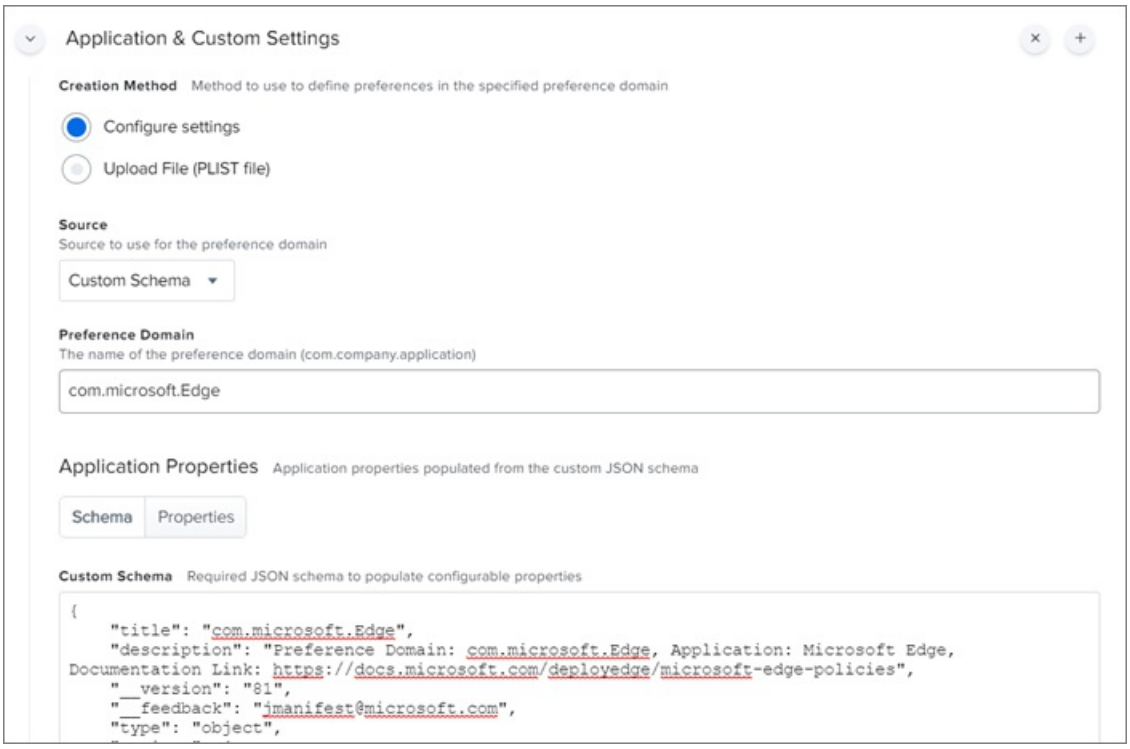
1. Sign in to Jamf.
2. Select the **Computer** tab.
3. Under **Content Management**, select **Configuration Profiles**.
4. On the **Configuration Profiles** page, click **+ New**.



5. On **New macOS Configuration Profile** > **Options**, select **Application & Custom Settings**.
6. On the **Application & Custom Settings** popup window, click **Configure**.

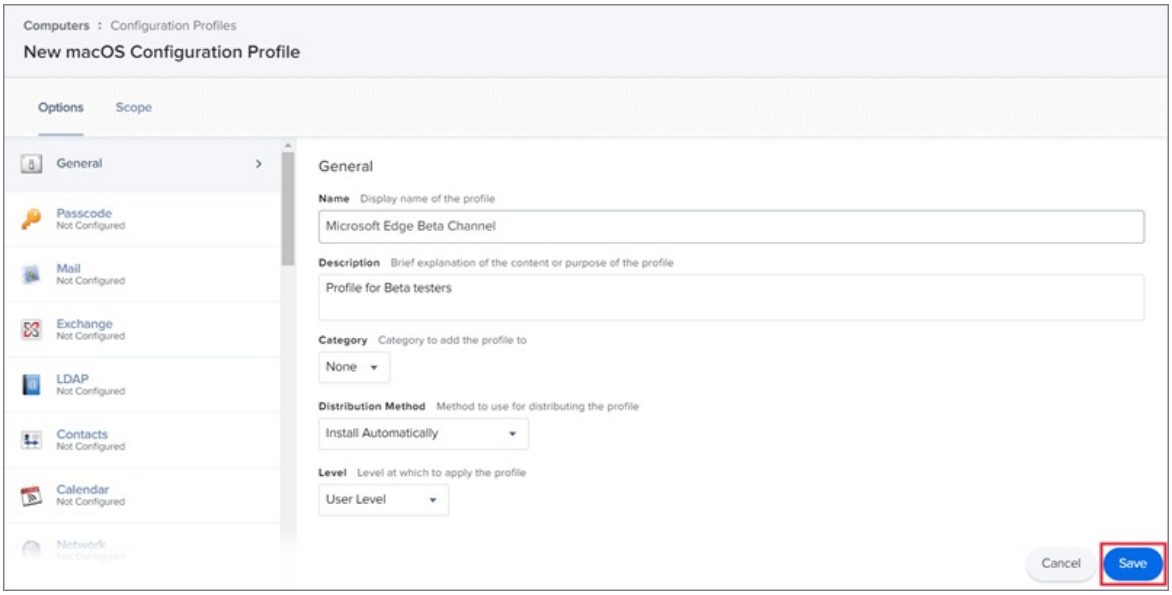


7. In the **Application & Custom Settings** section, set the values shown in the following screen shot.


Application & Custom Settings
Creation Method Method to use to define preferences in the specified preference domain
Configure settings
Upload File (PLIST file)
Source
Source to use for the preference domain
Custom Schema
Preference Domain
The name of the preference domain (com.company.application)
com.microsoft.Edge
Application Properties Application properties populated from the custom JSON schema
Schema
Properties
Custom Schema Required JSON schema to populate configurable properties
{
"title": "com.microsoft.Edge",
"description": "Preference Domain: com.microsoft.Edge, Application: Microsoft Edge,
Documentation Link: https://docs.microsoft.com/deployedge/microsoft-edge-policies",
"__version": "81",
"__feedback": "jmanifest@microsoft.com",
"type": "object",

- For **Creation Method**, pick **Configure settings**.
- For **Source**, pick **Custom Schema**.
- For **Preference Domain**, provide the name of your domain. This example uses *com.microsoft.Edge* as the domain.
- For **Custom Schema**, paste the contents of the "policy_manifest.json" manifest file.
- Click **Save**.

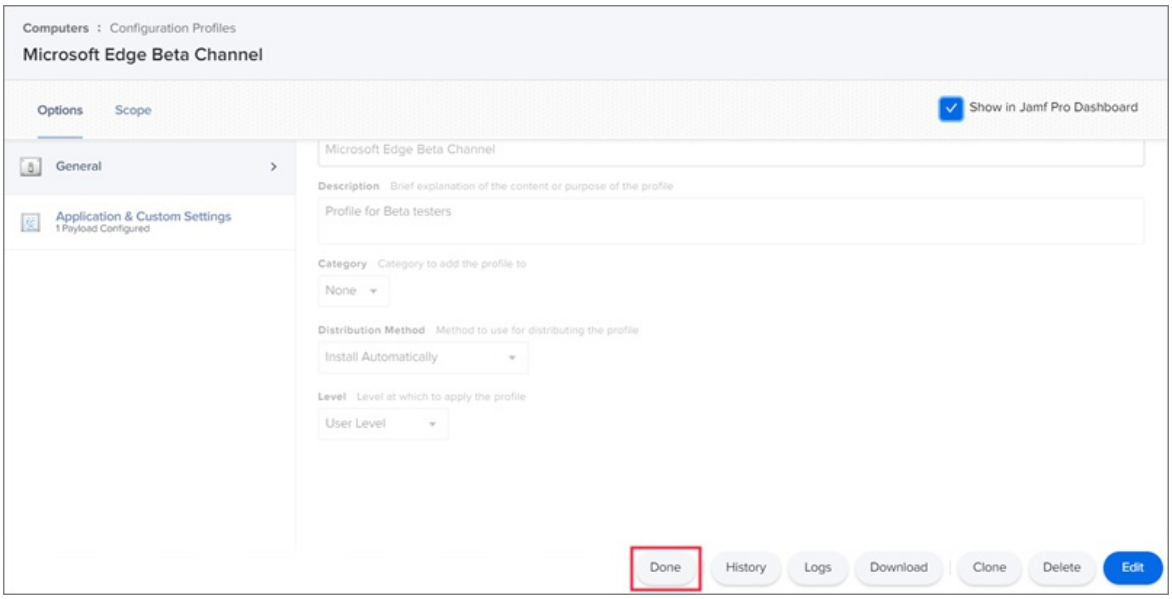
8. After you save the profile, Jamf displays the **General** section shown in the next screen shot.



- Provide a display **Name** for the profile and a **Description**.
- Keep the default setting for **Category**, which is **None**.
- For **Distribution Method**, the options are **Install Automatically** or **Make Available in Self Service**.
- For **Level**, the options are **User Level** or **Computer Level**.
- Click **Save**.

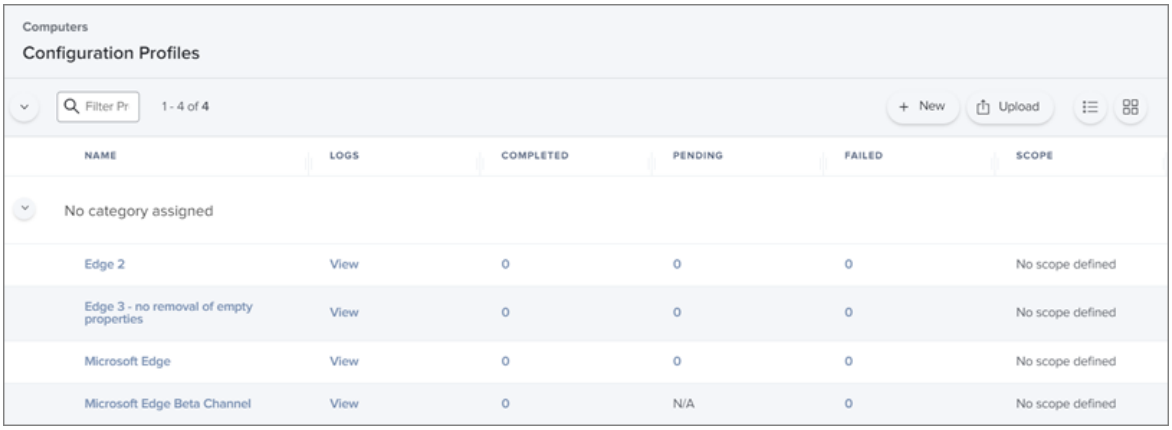
9. After you save the General section, Jamf shows the "Microsoft Edge Beta Channel" configuration profile set up for our example. In the next screen shot, note that you can keep working the profile by clicking

Edit or if you're finished, click **Done**.



> **NOTE**
>
> You can edit this profile after it's been saved and in another Jamf session. For example, you might decide to change the Distribution Method to Make Available in Self Service.

To do a follow up edit on the Microsoft Edge Stable Channel, or delete it, select the profile name, shown in the following Configuration Profiles screen shot.



After you create the new configuration profile you still have to configure the **Scope** for the profile.

To configure the scope

1. For **Targets**, provide the following minimum settings:
   - TARGET COMPUTERS. The options are Specific Computers or All Computers.
   - TARGET USERS. The options are Specific Users or All Users.
   - Click **Save**.
2. For **Limitations**, keep the default setting: None. Click **Cancel**.
3. For **Exclusions**, keep the default setting: None. Click **Cancel**.

See also

- Microsoft Edge Enterprise landing page
- Configure for macOS with Intune

- Configure for Windows
- Configure for Windows with Intune

Microsoft Edge Workspaces (Public Preview)

11/1/2022 • 5 minutes to read • Edit Online

This article describes the productivity benefits Edge Workspaces will bring to your users and how you can enable this feature and its functions in your organization.

> **NOTE**
> This is a preview feature. Preview features or services are in development and are available as a preview so you can get early access and send us feedback.

Overview

Edge Workspaces provides an incredible way for customers to organize their browsing tasks into dedicated windows. Each Edge Workspace contains its own sets of tabs and favorites, all created and curated by the user and their collaborators. Edge Workspaces are automatically saved and kept up to date. Workspaces are accessible anywhere customers use Microsoft Edge with their Azure Active Directory (Azure AD) accounts.

https://www.youtube.com/embed/bNRY9Zm1QY8

Edge Workspace scenarios

The following are key scenarios for using Edge Workspaces in your organization.

- Onboarding individuals to a project or working on projects with multiple teams can be difficult. With so many websites and files emailed back and forth, it's hard to keep up with everything. Instead of sharing links back and forth, you can create a workspace with a shared set of open websites and working files and send one link to quickly onboard a new individual or to make sure your team is on the same page.
- If an individual is working on multiple projects, they can create a workspace to organize the open tabs they have for each project. Whenever they want to work on that project, they can easily open its Edge Workspace and have everything they need in one place.

Prerequisites

- Users must have an Azure AD tenant and Microsoft Edge version 106 or greater installed.
- To enable via group policy, Admins must have Microsoft Edge version 106 or greater installed and version 107 of the policy files.
  - Edge Workspaces can also be enabled on a case-by-case basis using the Microsoft Edge flag: **#edge-workspaces**.
- Users must have access to a OneDrive for Business license to create an Edge Workspace.

> **IMPORTANT**
> Remember that each user in a shared Edge Workspace brings their own identity, authentication, and cookies to the open websites. A user might have access to a specific workspace, but might not have access to all the websites loaded in the workspace.

Enable workspaces for users

To enable Edge Workspaces for users in your organization, download the Microsoft Edge policy file (version

107.0.1402.2 or greater) and enable the EdgeWorkspacesEnabled policy. Eligible individuals can enable Edge Workspaces by enabling the **edge://flags#edge-workspaces** flag in Microsoft Edge.

> **NOTE**
> Native Microsoft Intune support for enabling Edge Workspaces will be available with Microsoft Edge version 107.

The Edge Workspaces user experience

Edge Workspaces lets users share a set of browser tabs so working groups can view the same websites and latest working files in one place and stay on the same page.

Imagine a scenario where a team member is being onboarded to a new project or is being added to a project in progress. Instead of sending multiple links back and forth over email, it's productive and convenient to share all the links as open tabs in a workspace. What's more, the user will be able to see which tab each group member is on and, if tabs are updated, will see those updates happen in real-time.

To learn more about how to get your users started with Edge Workspaces, visit: Getting started with Microsoft Edge Workspaces (public preview).

Workspaces sharing

A workspace shares the following information:

- The workspace's browser tabs, favorites, and history with your team in real time.
- The active tab for each group member that has the workspace open.

A workspace doesn't share the following information:

- A user's logins, passwords, downloads, collections, extensions, and cookies.
- Personal browser settings such as appearance or search engine.
- Any tabs or data from outside the workspace.
- Website content that only the user can access. For example, if the user logs in to their email in a shared Edge Workspace, only the user will see their email content.
- A user's device screen. Users sharing a workspace won't see how other users interact with an open website or website content that they don't have access to.

Providing feedback

Your feedback while using Edge Workspaces is valuable to help us improve the product!

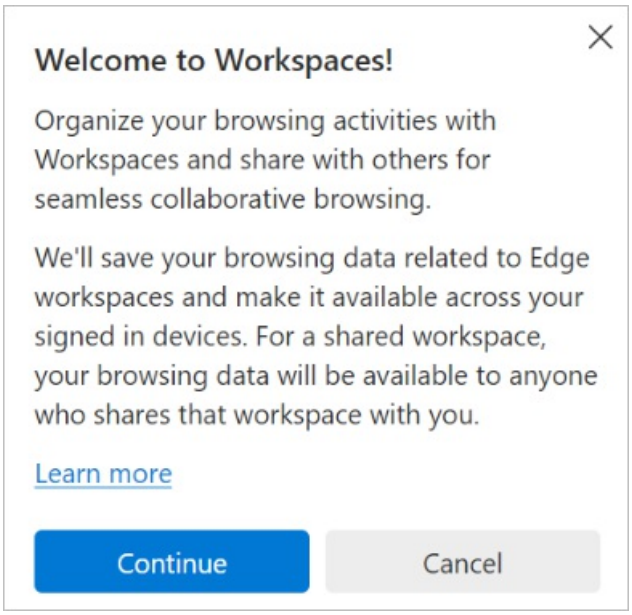
You can leave feedback by clicking the **Like** or **Dislike** button at the bottom of the Edge Workspace menu. These buttons are next to the question: "Are you satisfied with Workspaces?".

> **NOTE**
> While in preview, this experience is supported by Microsoft Support, and customers with Premier support can leverage this to report any feedback, or concerns.

Frequently Asked Questions

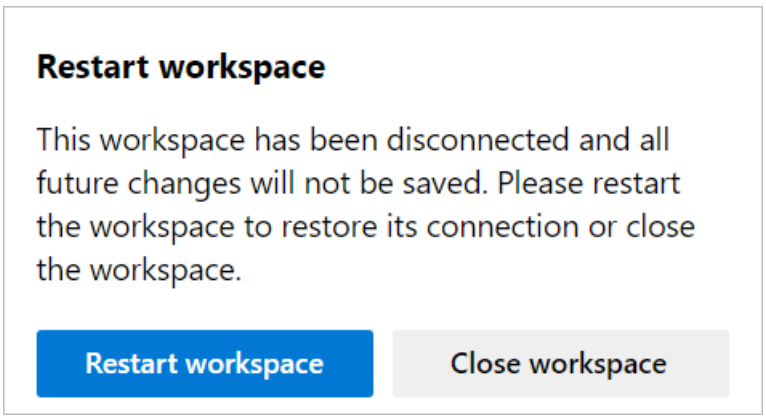
My users got the following message when they opened Edge Workspaces for the first time. What does this message mean and what should they do?

This message is shown the first time a user clicks the Workspaces menu in the browser. They have the option to get more information or click **Continue** to create a workspace.


Welcome to Workspaces!
Organize your browsing activities with Workspaces and share with others for seamless collaborative browsing.
We'll save your browsing data related to Edge workspaces and make it available across your signed in devices. For a shared workspace, your browsing data will be available to anyone who shares that workspace with you.
Learn more
Continue
Cancel

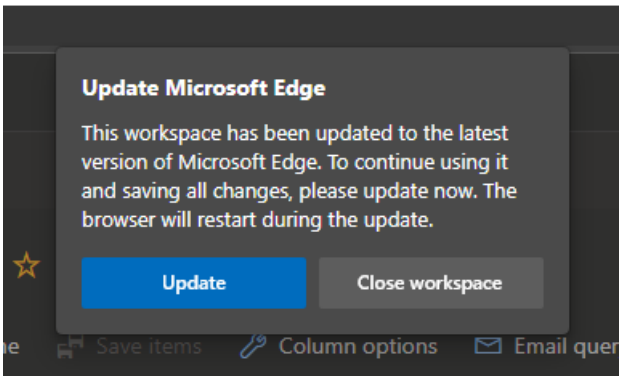
I see the "Restart workspace" message. Why do I see this message and what should I expect?

This is due to a temporary connectivity issue because Microsoft Edge can't connect to the service that provides and supports Edge Workspaces.


Restart workspace
This workspace has been disconnected and all future changes will not be saved. Please restart the workspace to restore its connection or close the workspace.
Restart workspace
Close workspace

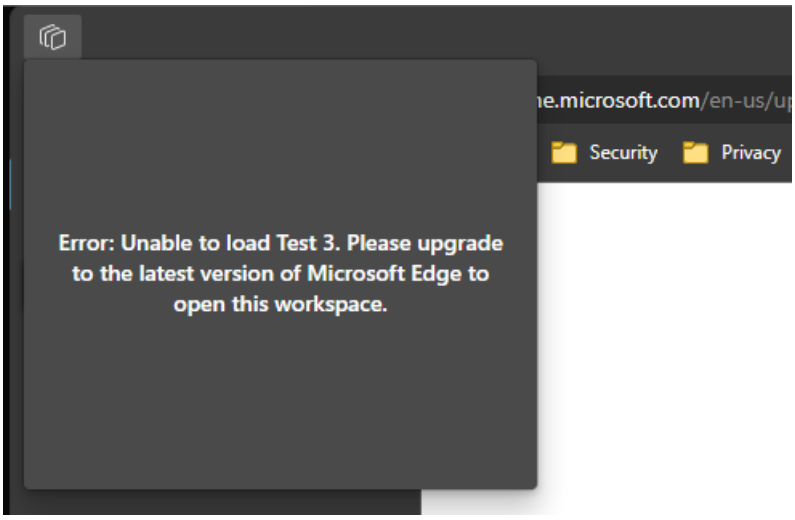
I see the "Update Microsoft Edge" message. Why do I see this message and what should I expect?

The Edge Workspaces software was updated and you need to update Microsoft Edge to keep using your workspaces.


Update Microsoft Edge
This workspace has been updated to the latest version of Microsoft Edge. To continue using it and saving all changes, please update now. The browser will restart during the update.
Update
Close workspace
Save items
Column options
Email quer

My user got the following error. What should they do?

The Edge Workspaces software was updated and you need to update Microsoft Edge to keep using your workspaces.


e.microsoft.com/en-us/u
Security
Privacy
Error: Unable to load Test 3. Please upgrade to the latest version of Microsoft Edge to open this workspace.

Can I lock down an Edge workspace after I share it (Read-only) so that I'm the only one who can close or open tabs?

No. Right now, anyone whom the Edge Workspace is shared with can open or close any tab. If someone closes a tab you want to keep, you can always reopen it as a new tab.

If I close a tab in a workspace, does that close it for everyone in the workspace?

Yes. Tabs in Edge Workspaces are shared in real-time for everyone. If someone closes a tab, it closes that tab for everyone that's using the workspace.

Where is my workspace data stored and how is it protected?

Workspace data is stored in your personal OneDrive for business and carries the same protections as all the other content stored in OneDrive.

See also

- Microsoft Edge Enterprise landing page

Microsoft Edge for Virtual desktop infrastructure (VDI)

11/1/2022 • 5 minutes to read • Edit Online

This article describes the requirements and limitations for using Microsoft Edge in a virtual environment.

What is VDI?

Virtual desktop infrastructure (VDI) is a desktop virtualization technology that hosts an operating system and applications on a centralized server in a data center. This technology enables a fully personalized desktop experience for users on a secure and compliant centralized source.

Microsoft Edge can be used in a virtual environment in much the same way as it's used on a local device. A virtual desktop takes advantage of a secure and controlled server environment. Depending on the VDI solution you choose, it might also be possible to give your users seamless access to intranet applications and sites.

Most Microsoft Edge features are supported in VDI environments without any special configuration. However, to ensure an optimal experience we recommend that you review the following guidance.

Platforms certified for Microsoft Edge

The following platforms are certified for Microsoft Edge:

- Azure Virtual Desktop
- Citrix Virtual Apps and Desktops (formerly known as XenApp and XenDesktop)

Although other VDI solutions haven't been certified by the Microsoft Edge team yet, it's expected that the most common workflows in Microsoft Edge should be supported. The following guidance may or may not be applicable to your chosen solution.

Performance considerations for Microsoft Edge on VDI

When designing your VDI environment you should carefully consider the workflows and needs of your users to achieve optimal performance, and understand the limits of your server configuration.

The following minimum requirements are recommended for deploying Microsoft Edge on a VDI environment:

- vCPU – 2-4 cores per User
- RAM – 1 GB per User

Large and complex web applications and extensions will need more memory and processing capability, which must be considered when configuring your virtual environment.

Microsoft Edge on non-persisted VDI environments

Many VDI solutions allow access to persisted environments, where users are assigned a virtual environment that persists between sessions, and non-persisted environments, where users are assigned to one of several available machines, possibly a different machine each session, user data may or may not sync between sessions.

When using a non-persisted environment, one usually creates a "golden image" that has the required apps and configurations that will be deployed on each device. Use the following recommendations as a guide for preparing a golden image.

Deploy Microsoft Edge

If you are on Windows 10, version 1803 and above, you should already have Microsoft Edge installed on your system. However, if you're using an older version of Windows or want to deploy a different Microsoft Edge channel, follow these steps:

1. Download the Microsoft Edge MSI package that matches your VDI VM operating system from:
   - Download Microsoft Edge for Business - Microsoft
2. Run the following command to install the MSI to the VDI virtual machine (VM):
   - `msiexec /i <path_to_msi> /qn /norestart /l*v <install_logfile_name>`

Disable automatic updates

For non-persisted machines, the best practice to disable automatic updates and update Microsoft Edge by updating the golden image to ensure that there are no version mismatches among the pool of virtual machines.

For more information about disabling automatic updates, see the following policies:

- Update policy override default
- Update policy override

Profile management

On non-persisted setups, it's important to consider that VMs may not maintain user state between sessions or users may be assigned a VM they've never used before. In this scenario, the VM doesn't have any of the user's data.

Microsoft Edge supports several methods for syncing user data so it's available regardless of how they are accessing Microsoft Edge. Two methods are Azure Active Directory (Azure AD) sync and on-premises sync for AD users.

Azure AD Sync

If your Azure AD plan supports it, Enterprise sync is the fastest and easiest method to ensure that Microsoft Edge user data is synced to all user devices. For more information, see Configure Microsoft Edge enterprise sync

On-premise Sync for Active Directory Users

With on-premises sync, Microsoft Edge saves an Active Directory user's favorites and settings to a file that can easily be moved between different computers.

For more information about requirements and configuration, see On-premises sync for Active Directory (AD) users

User Profile Redirection

There are several solutions for migrating and redirecting the entire user folder to ensure that user context is maintained in a non-persisted environment. Check with your VDI provider to determine the recommended solution for your environment.

Some popular solutions include the following options:

- FSLogix Overview - FSLogix
- How to Configure Citrix Profile Management

It some cases, unnecessary folders should be excluded from the backed-up user folder to reduce initial loading times when a user's logging on to a machine and their profile is being migrated. If so, we recommend the following folders be excluded from your backup to reduce size.

- %LocalAppData%\Microsoft\Edge\User Data\Default\Cache

- %LocalAppData%\Microsoft\Edge\User Data\Default\Code Cache
- %LocalAppData%\Microsoft\Edge\User Data\Default\JumpListIconsTopSites
- %LocalAppData%\Microsoft\Edge\User Data\Default\JumpListIconsRecentClosed

Known issues

Microsoft Edge crashes in older versions of XenApp and XenDesktop

This issue should be mitigated in newer versions of these products. However, if you're encountering this issue in your environment, you can work around the issue by disabling Citrix API Hooks for Microsoft Edge, see How to Disable Citrix API Hooks on a Per-application Basis.

Degraded performance when rendering pages with exceptionally large HTML tables

The following Citrix policies are known to slow rendering of html pages with large (30,000+ row) tables.

- Automatic keyboard display
- Remote the combo box

For more information, see Mobile experience policy settings (citrix.com) for more information. Disabling these policies should mitigate the issue.

Windows Account Manager authorization scenarios (that is, Azure sync) fail in Microsoft Edge when run as a Citrix seamless application

This is a known issue in Microsoft Edge and other applications that use WAM (that is, Office) due to necessary Windows components not being initialized when running in the "seamless" mode. Try one of the following options to work around this issue:

- Use Microsoft Edge via a Remote Desktop to the Citrix Host instead of a seamless remote application.
- Use Azure Virtual Desktop remote apps instead, which has mitigations for this issue.

See also

- Microsoft Edge Enterprise landing page
- Azure Virtual Desktop

Microsoft Edge configurations and experimentation

11/1/2022 • 2 minutes to read • Edit Online

This article describes the interaction between Microsoft Edge and the Experimentation and Configuration Service (ECS). Microsoft Edge communicates with this service to request and receive different kinds of payloads. These payloads include configurations, feature rollouts, and experiments.

IMPORTANT

Make sure clients are able to access `https://config.edge.skype.com` so payloads can be received.

NOTE

This applies to Microsoft Edge version 77 or later.

Configurations

Configurations are the payload meant to ensure product health, security, and privacy compliance, and are intended to have the same value for all the users (based on platforms and channels.) This could be to enable a feature flag for a domain action, and can also be used to disable a feature flag in the event of a bug.

Controlled Feature Rollout

Controlled Feature Rollout (CFR) is a procedure for slowly increasing the size of the user group that receives a feature. By distributing a new feature to a randomly selected subset of the user population, it's possible to compare user feedback to an equally sized control group without the feature to measure the impact of the feature.

Experiments

Microsoft Edge builds have features and functionality that are still in development or are experimental. Experiments are like CFR, but the size of the user group is much smaller for testing the new concept. These features are hidden by default until the feature's rolled out or the experiment's finished. Experiment flags are used to enable and disable these features.

About the ECS

In all the preceding scenarios, the service delivers the feature flag values to the browser client so they can be applied. Depending on the update, configurations are applied immediately or when the user restarts the browser.

Microsoft Edge's interaction with this service is controlled by settings in the ExperimentationAndConfigurationServiceControl policy. You can configure policy settings to:

- Retrieve configurations only
- Retrieve configurations and experiments
- Disable communication with the service

Caution

If you disable communications with the service, this will affect Microsoft's ability to respond to a severe bug in a timely manner.

See also

- Microsoft Edge Enterprise landing page
- Microsoft Edge documentation landing page

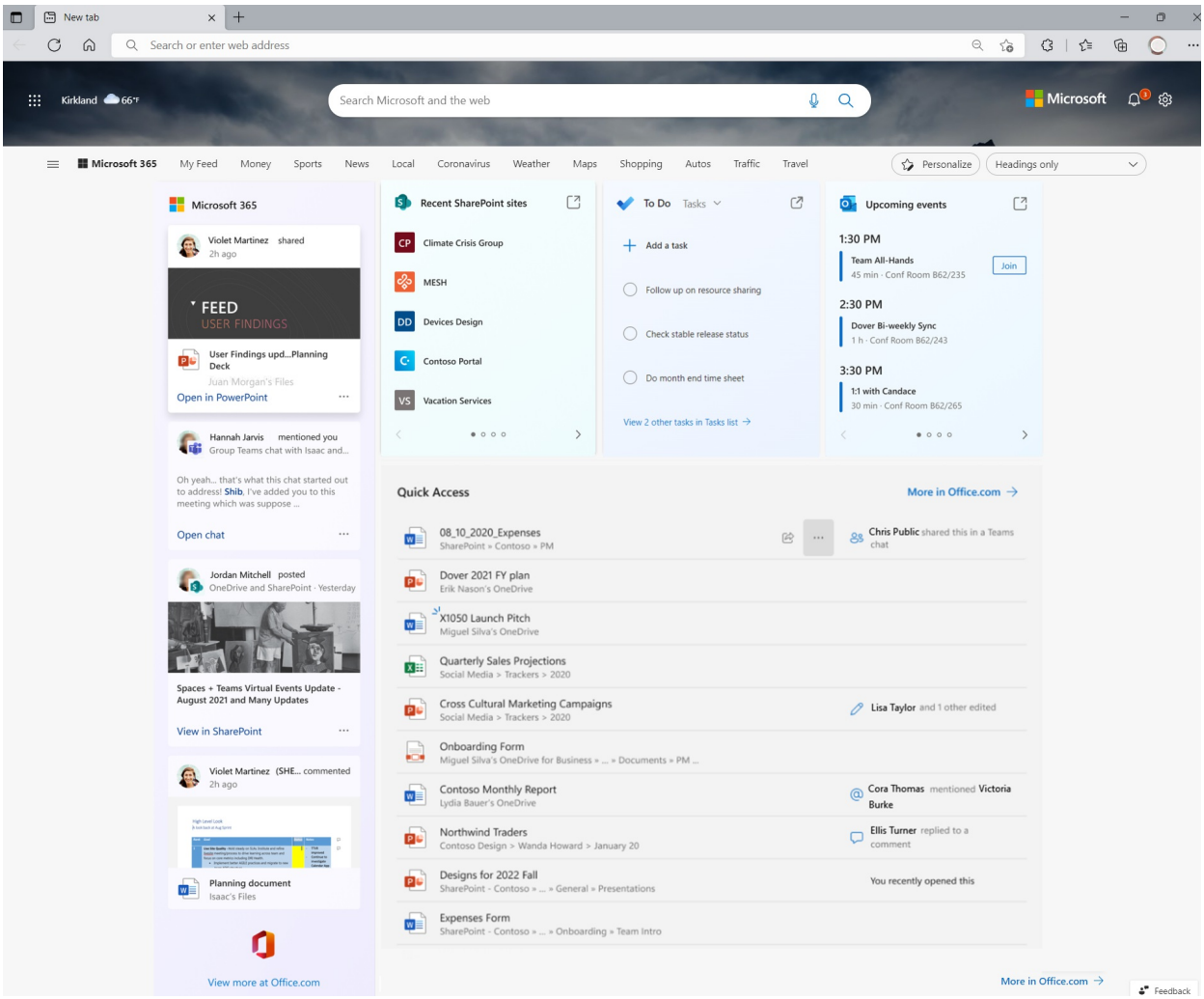
Microsoft Edge Enterprise new tab page

11/1/2022 • 4 minutes to read • Edit Online

The Enterprise new tab page is a direct response to a new challenge that workers face daily: frequent context switching. Our research shows that in addition to managing schedules, workers juggle roughly three projects a day—and on average, switch between them two to three times a day. Combine that switching with a torrent of emails, pings, and calls (which, when combined, can easily number in the triple digits) and they're constantly switching contexts throughout their day. Finally, add on the challenge of hybrid workplaces and it's no wonder they want to work smarter not harder.

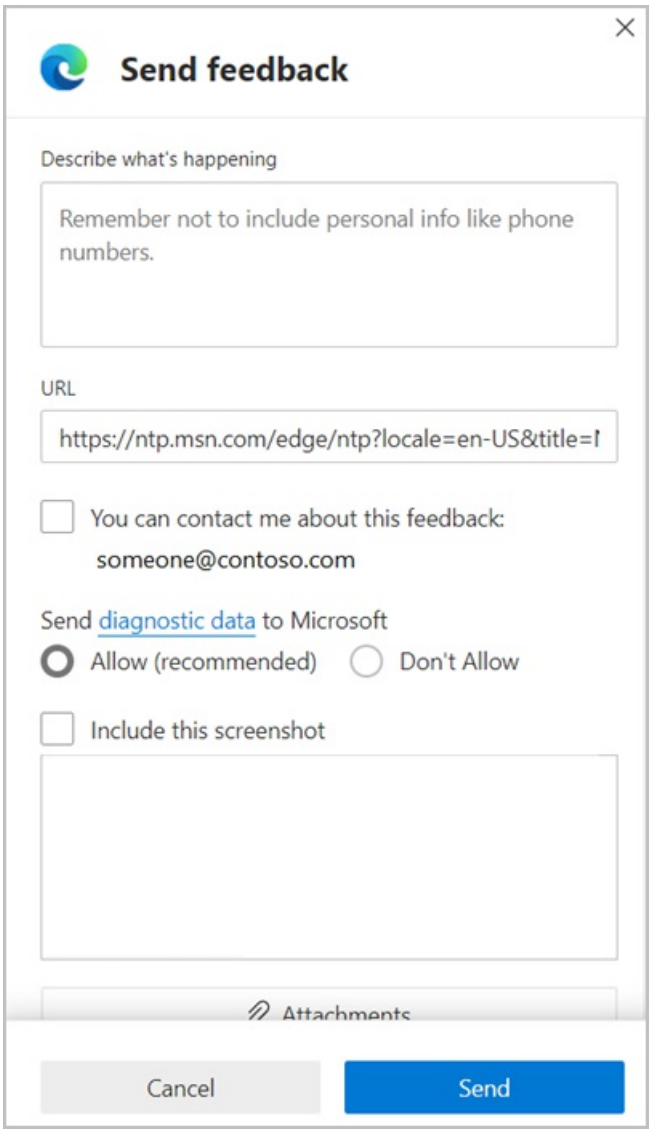
The role of the browser

As the browser role grows to become central for workers to finish everyday tasks, it's more important now than ever that information workers can cut through the noise and find what they need. That's why we've created a personalized productivity dashboard right in the Microsoft Edge Enterprise new tab page. Any enterprise user of Microsoft Edge can use this by opening a new tab and then selecting the **Microsoft 365** tab.



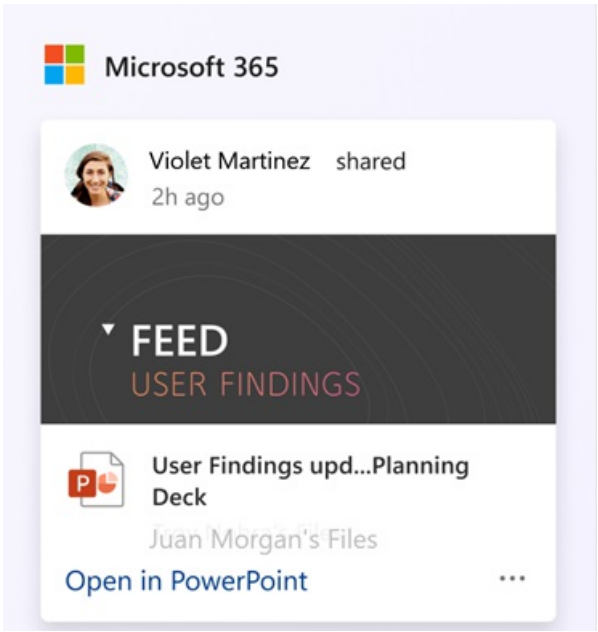
The dashboard is a focal point for quickly finding the information you need and stay up to date on the things that matter most, all while cutting out the noise. Now, we'll highlight some of the top features that can help keep your employees productive.

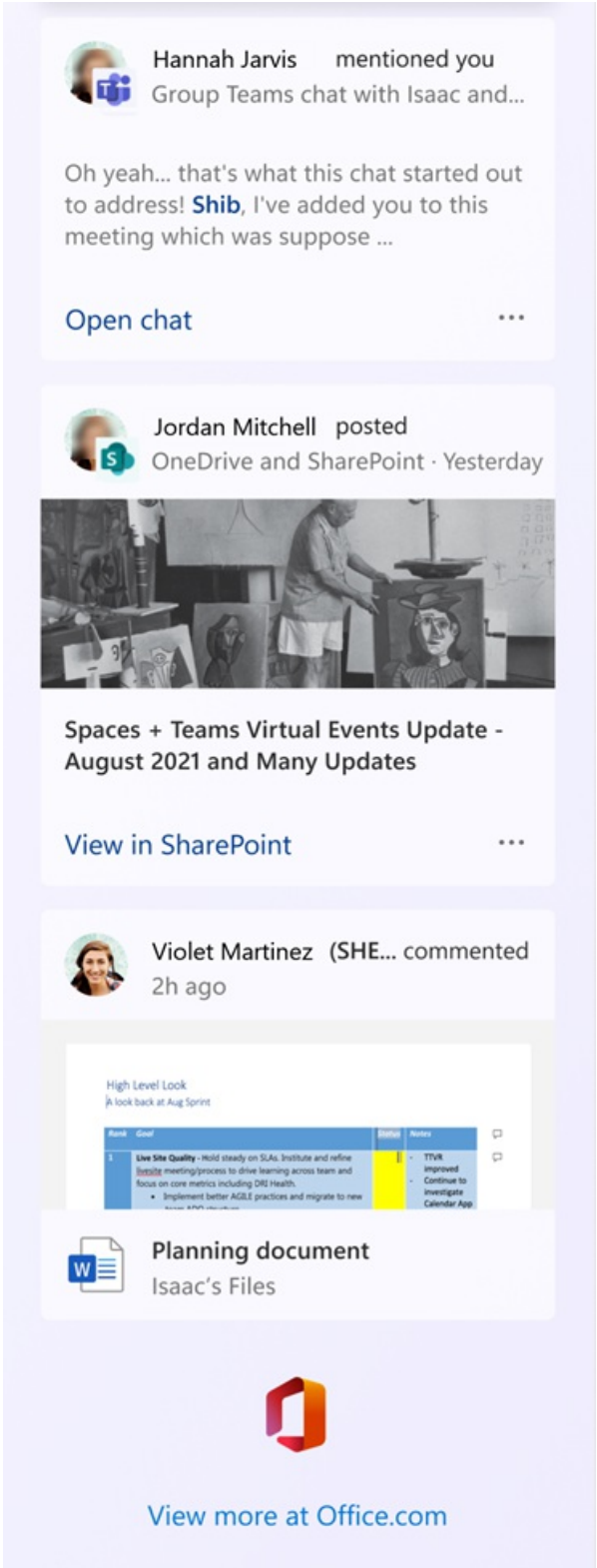
We're continuously looking to improve the browser experience so we want to get your feedback, which you can provide by pressing alt + shift + I to open the **Send feedback** dialog where you can share your thoughts.



Microsoft 365 feed

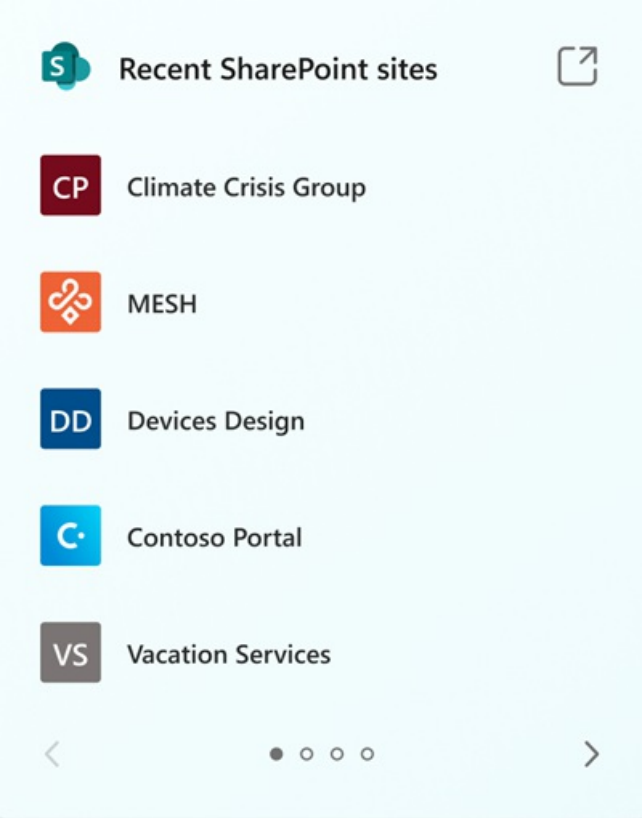
Do you feel overwhelmed by trying to keep up with all the updates at work? The Microsoft 365 feed is personalized to you and your work. This feed uses Microsoft 365 data to bring you the most important information happening around your organization. From at mentions, to files being edited, to meeting recordings you might want to catch-up on, to colleague promotions, and so much more. This experience helps keep you up to date on the most important information at a glance.




Hannah Jarvis mentioned you
Group Teams chat with Isaac and...
Oh yeah... that's what this chat started out to address! Shib, I've added you to this meeting which was suppose ...
Open chat
Jordan Mitchell posted
OneDrive and SharePoint · Yesterday
Spaces + Teams Virtual Events Update - August 2021 and Many Updates
View in SharePoint
Violet Martinez (SHE... commented
2h ago
High Level Look
A look back at Aug Sprint
Planning document
Isaac's Files
View more at Office.com

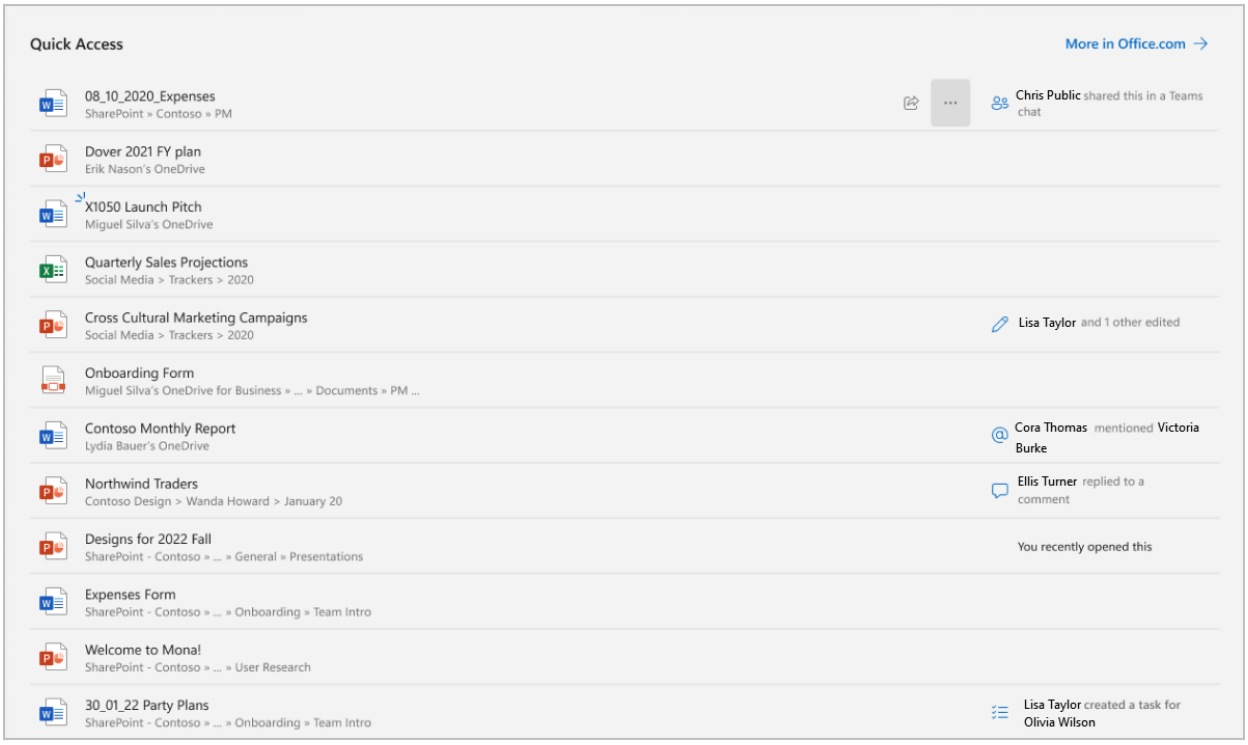
Recent SharePoint sites card

Tired of jumping through hoops to get to your SharePoint sites? Here's a shortcut to help you get the information you need to be productive, even faster.



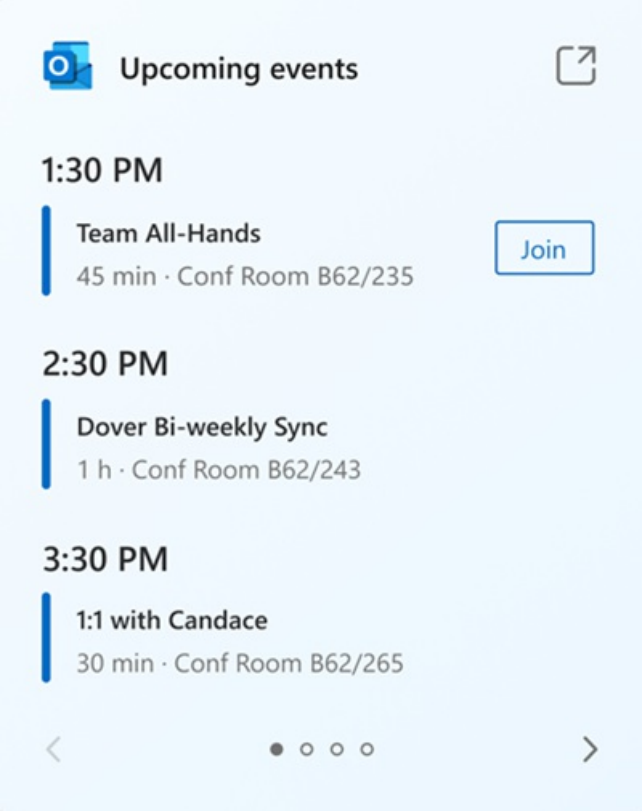
Quick Access list

Our research shows that information workers can handle tens, if not hundreds of files over a given week. This volume can get overwhelming when you don't know where each file is saved or who sent it to you. This module ranks files we think are most important to you to help you find them quickly. Don't see them here? That's okay, you can either use our new Work Search features (information later) to look up the file name or the name of the colleague who sent it to you, or use the **More in Office.com** link at the bottom of the list to hop to Office.com and find it there.


Quick Access
More in Office.com
08_10_2020_Expenses
SharePoint » Contoso » PM
Chris Public shared this in a Teams chat
Dover 2021 FY plan
Erik Nason's OneDrive
X1050 Launch Pitch
Miguel Silva's OneDrive
Quarterly Sales Projections
Social Media > Trackers > 2020
Cross Cultural Marketing Campaigns
Social Media > Trackers > 2020
Lisa Taylor and 1 other edited
Onboarding Form
Miguel Silva's OneDrive for Business » ... » Documents » PM ...
Contoso Monthly Report
Lydia Bauer's OneDrive
Cora Thomas mentioned Victoria Burke
Northwind Traders
Contoso Design > Wanda Howard > January 20
Ellis Turner replied to a comment
Designs for 2022 Fall
SharePoint - Contoso » ... » General » Presentations
You recently opened this
Expenses Form
SharePoint - Contoso » ... » Onboarding » Team Intro
Welcome to Mona!
SharePoint - Contoso » ... » User Research
30_01_22 Party Plans
SharePoint - Contoso » ... » Onboarding » Team Intro
Lisa Taylor created a task for Olivia Wilson

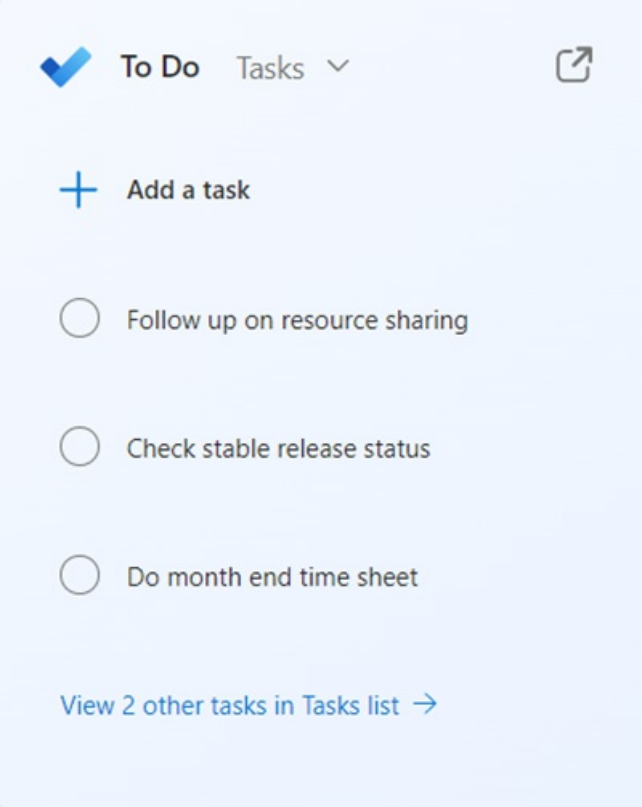
Upcoming events card

One of the most important aspects of keeping up with a fast-paced work environment is knowing what meetings you have coming up and when they're scheduled. As if it wasn't hard difficult enough to begin with, hybrid work has increased the number of meetings for many workers, causing overload. No productivity dashboard is complete without a glanceable calendar to make sure you're prepared for your meetings. And with one click you can join your Teams meeting or send a message to other attendees if you happen to be running late.



To Do task list

One of the most effective ways for many users to stay productive when they're getting overwhelmed is to make a to do list. This keeps users organized and can be cathartic to check items off the list when they are feeling stressed. We have To Do integration in the browser so you can get all the greatness of Microsoft To Do in an easily accessible format.



Address bar

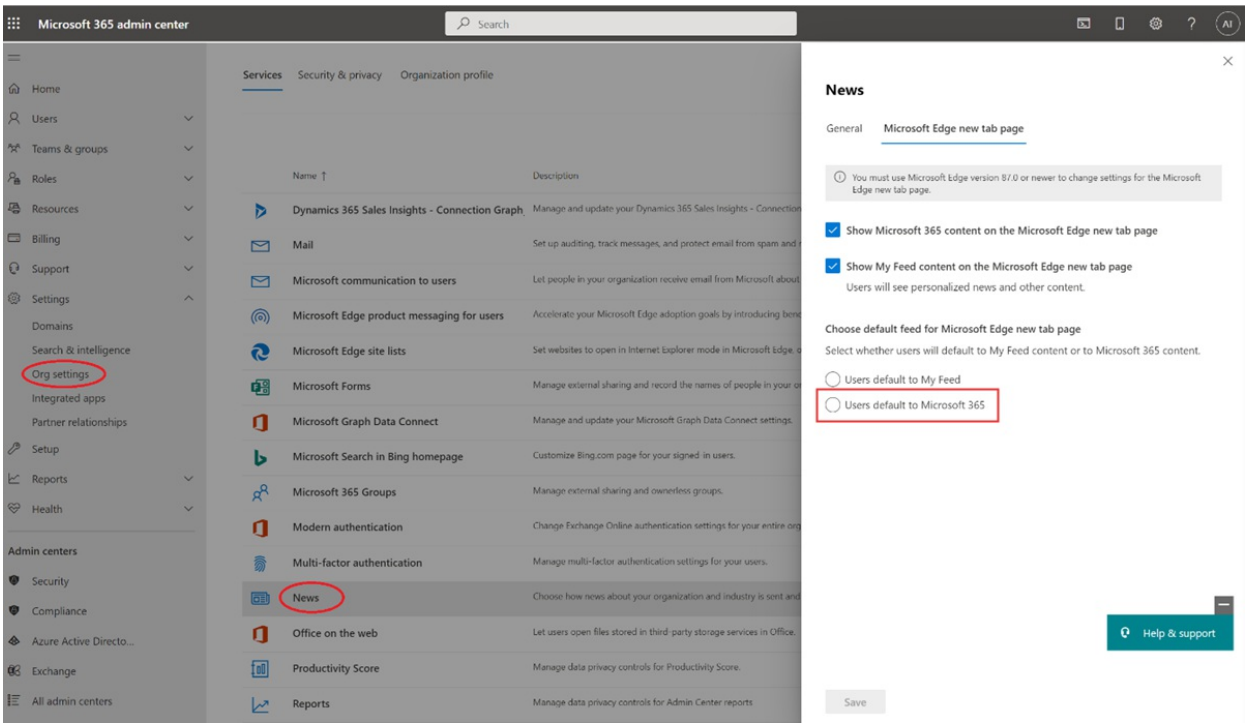
Trying to find something for work, but can't quite figure out where to start? Just search for it! The Microsoft Edge address bar (location bar or URL bar) supports finding work content through Microsoft Search for Bing (MSB). Type your query and search or select one of the auto-suggested work results in Microsoft Suggests. You can also select "my organization" in the Microsoft search banner for work information only.

How to make Microsoft 365 the default tab

If you're a user, click the **Microsoft 365** tab at the bottom of your new tab page in Microsoft Edge and when you return to the page it should be set as the default!

For tenant admins, if you'd like to have your organization automatically set Microsoft 365 as the default tab, follow these steps:

1. Sign in to the Microsoft 365 admin center.
2. Go to **Org settings** > **News**.
3. Under **News**, **select Microsoft Edge new tab page**.
4. Select the toggle in the next screenshot that says "Users default to Microsoft 365".



See also

- Microsoft Edge Enterprise landing page

Microsoft Edge identity support and configuration

11/1/2022 • 5 minutes to read • Edit Online

This article describes how Microsoft Edge uses identity to support features such as sync and single sign-on (SSO). Microsoft Edge supports signing in with Active Directory Domain Services (AD DS), Azure Active Directory (Azure AD), and Microsoft accounts (MSA). Currently, Microsoft Edge only supports Azure Active Directory (Azure AD) accounts belonging to the global cloud or the GCC sovereign cloud. We're working on adding support for other sovereign clouds.

> **NOTE**
> This applies to Microsoft Edge version 77 or later.

Browser sign-in and authenticated features

Microsoft Edge supports signing into a browser profile with an Azure AD, MSA, or a domain account. The type of account used for sign-in determines which authenticated features are available for the user in Microsoft Edge. The following table summarizes the feature support for each type of account.

FEATURE	AZURE AD PREMIUM	AZURE AD FREE	ON-PREMISES AD DS	MSA
Sync	Yes	No	No	Yes
SSO with Primary Refresh Token	Yes	Yes	No	Yes
Seamless SSO	Yes	Yes	Yes	N/A
Integrated Windows Authentication	Yes	Yes	Yes	N/A
Enterprise New tab page	Requires O365	Requires O365	No	N/A
Microsoft Search	Requires O365	Requires O365	No	N/A

How users can sign into Microsoft Edge

Automatic sign-in

Microsoft Edge uses the OS default account to auto sign into the browser. Depending on how a device is configured, users can get auto signed into Microsoft Edge using one of the following approaches.

- **The device is hybrid/AAD-J:** Available on Win10, down-level Windows, and corresponding server versions. The user gets automatically signed in with their Azure AD account.
- **The device is domain joined:** Available on Win10, down-level Windows, and corresponding server versions. By default, the user won't get automatically signed in. If you want to automatically sign in users with domain accounts, use the ConfigureOnPremisesAccountAutoSignIn policy. If you want to automatically sign in users with their Azure AD accounts, consider hybrid joining your devices.
- **OS default account is MSA:** Win10 RS3 (Version 1709/Build 10.0.16299) and above. This scenario is

unlikely on enterprise devices. But, if the OS default account is MSA, Microsoft Edge will sign in automatically with the MSA account.

Manual sign-in

If the user doesn't get automatically signed into Microsoft Edge, they can manually sign into Microsoft Edge during the first run experience, browser settings, or by opening the identity flyout.

Managing browser sign-in

If you want to manage browser sign-in, you can use the following policies:

- Ensure that users always have a work profile on Microsoft Edge. See NonRemovableProfileEnabled
- Restrict sign-in to a trusted set of accounts. See RestrictSigninToPattern
- Disable or force browser sign-in. See BrowserSignin

Browser to Web Single Sign-On (SSO)

On some platforms, you can configure Microsoft Edge to automatically sign into websites for your users. This option saves them the trouble of reentering their credentials to access their work websites and increases their productivity.

SSO with Primary Refresh Token (PRT)

Microsoft Edge has native support for PRT-based SSO, and you don't need an extension. On Windows 10 RS3 and above, if a user is signed into their browser profile, they'll get SSO with the PRT mechanism to websites that support PRT-based SSO.

A Primary Refresh Token (PRT) is an Azure AD key that's used for authentication on Windows 10, iOS, and Android devices. It enables single sign-on (SSO) across the applications used on those devices. For more information, see What is a Primary Refresh Token?.

Seamless SSO

Just like PRT SSO, Microsoft Edge has native Seamless SSO support without needing an extension. On Windows 10 RS3 and above, if a user is signed into their browser profile, they'll get SSO with the PRT mechanism to websites that support PRT-based SSO.

Seamless Single Sign-On automatically signs users in when they're on corporate devices connected to a corporate network. When enabled, users don't need to type in their passwords to sign in to Azure AD. Typically they don't even have to type in their usernames. For more information, see Active Directory Seamless Single Sign-On.

Windows Integrated Authentication (WIA)

Microsoft Edge also supports Windows Integrated Authentication for authentication requests within an organization's internal network for any application that uses a browser for its authentication. This is supported on all versions of Windows 10 and down-level Windows. By default, Microsoft Edge uses the intranet zone as an allowlist for WIA. Alternatively, you can customize the list of servers that are enabled for Integrated Authentication by using the AuthServerAllowlist policy. On macOS, this policy is required to enable Integrated Authentication.

To support WIA-based SSO on Microsoft Edge (version 77 and later), you might also have to do some server-side configuration. You'll probably have to configure the Active Directory Federation Services (AD FS) property **WiaSupportedUserAgents** to add support for the new Microsoft Edge user agent string. For instructions on how to do this, see View WIASupportedUserAgent settings and Change WIASupportedUserAgent settings. An example of the Microsoft Edge user agent string on Windows 10 is shown below, and you can learn more about the Microsoft Edge UA string here.

The following example of a UA string is for the latest Dev Channel build when this article was published:

```
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3951.0
Safari/537.36 Edg/80.0.334.2"
```

For services that require delegating Negotiate credentials, Microsoft Edge supports Constrained Delegation using the AuthNegotiateDelegateAllowlist policy.

Additional authentication concepts

Proactive Authentication

Proactive authentication is an optimization over browser to website SSO that front loads authentication to certain first party websites. This improves address bar performance if the user is using Bing as the search engine. This gives users personalized and Microsoft Search for Business (MSB) search results. It also enables allowing authentication to key services such as the Office New Tab Page.

> **NOTE**
> If you want to configure browser sign in after version 90, use the BrowserSignin policy. For Microsoft Edge version 90 or lower, you can control this service using the ProactiveAuthEnabled policy.

Windows Hello CredUI for NTLM Authentication

When a website tries to sign users in using the NTLM or Negotiate mechanisms and SSO isn't available, we offer users an experience where they can share their OS credentials with the website to satisfy the authentication challenge using Windows Hello Cred UI. This sign-in flow will only appear for users on Windows 10 who don't get single-sign-on during an NTLM or Negotiate challenge.

Sign in automatically using saved passwords

If a user saves passwords in Microsoft Edge, they can enable a feature that automatically logs them into websites where they have saved credentials. Users can toggle this feature by navigating to *edge://settings/passwords*. If you want to configure this ability, you can use the password manager policies.

See also

- Microsoft Edge Enterprise landing page
- Video: Microsoft Edge and Identity
- Identity and access management
- Identity platform
- Four steps to a strong identity foundation with Azure Active Directory

Microsoft Edge and Enterprise State Roaming

11/1/2022 • 4 minutes to read • Edit Online

This article explains how Microsoft Edge participation in the Enterprise State Roaming (ESR) offering is changing to better support sync across platforms and devices.

> **NOTE**
> This article applies to Microsoft Edge version 77 or later unless otherwise noted.

Introduction

With Windows 10, Azure Active Directory (Azure AD) users gained the ability to securely synchronize their user settings and application settings data to the cloud. Enterprise State Roaming (ESR) provides users with a unified experience across their Windows devices and reduces the time needed for configuring a new device.

As a result of Microsoft Edge adopting the Chromium platform, its sync solution is now disconnected from Windows sync framework. This disconnect affects the relationship of Microsoft Edge to the ESR offering.

> **IMPORTANT**
> Microsoft Edge does not participate in the ESR offering.

What's changing with Microsoft Edge?

With Microsoft Edge, the sync solution isn't tied to the Windows sync ecosystem. This sync solution lets us offer Microsoft Edge across all the platforms, such as Windows 7, Windows 8.1, iOS, Android and macOS. We're also able to offer sync for non-primary accounts on Windows. In addition, we can ship Microsoft Edge at a more frequent and flexible release cadence than Windows. (For more information, see Windows updates to support the next version of Microsoft Edge. All these factors highlighted the need to reassess Microsoft Edge participation in the ESR offering.

ESR is framed as a Windows product offering with promises about how data from Windows devices is handled, but Microsoft Edge sync will extend this functionality beyond Windows devices. Because the data roams across these devices, it makes it difficult to define the Microsoft Edge sync offering in the context of ESR. To simplify how sync works and is managed, and to accommodate the changes that are highlighted, a decision was made to pull Microsoft Edge out of the ESR offering.

Does this mean that Enterprises will lose the abilities they had as part of ESR?

No. Microsoft Edge will continue to support most of the abilities provided in the ESR offering.

Unified experience across devices and new device configuration time

When a user is signed into their windows device with an Azure Active Directory (Azure AD account), Microsoft Edge will implicitly inherit that Identity on first launch of the new browser.

After a user has explicitly consented to turn on sync in Microsoft Edge, the browser will sync all the browser data, such as favorites, passwords, and history. Sync ensures a unified experience across devices and reduces the

time needed to personalize the browser.

Separation of corporate and consumer data

Organizations are in control of their data, and there's no mixing of corporate data in a consumer cloud account or consumer data in an enterprise cloud account.

Enhanced security

Data is automatically encrypted before leaving the user's Windows 10 device by using Azure Information Protection, and data stays encrypted at rest in the cloud. All content stays encrypted at rest in the cloud, except for the namespaces, like settings names.

Monitoring

We'll provide control and visibility over who syncs settings in your organization and on which devices through integration with the Azure AD portal. This capability will be enabled in a future release.

Management

Admins will be able to control which members in your organization can enable sync. See Use Azure Information Protection to configure Microsoft Edge sync and Sync group policies. Additionally, users can turn sync on/off for each of their devices and toggle each data attribute individually for sync.

Key management

The synchronization feature uses Azure Information Protection (AIP) to protect the synchronized data for only the user and the enterprise admins. AIP supports Microsoft managed keys (default) and bring your own key for cloud-key management. The cloud-key management strategy your organization uses is transparent to Microsoft Edge and has no impact on the synchronization feature.

> **IMPORTANT**
> Hold your own key (HYOK) and the Active Directory Rights Management Service aren't supported.

Summary of sync attributes

The following data attributes will sync in the new version of Microsoft Edge at first launch:

- Favorites
- Passwords
- Addresses and more (form-fill)
- Collections
- Settings
- Extensions
- Open tabs (available in Microsoft Edge version 88 or later)
- History (available in Microsoft Edge version 88 or later)

The preceding list of attributes is different than the attributes that could be synced in Microsoft Edge Legacy. (For details about Microsoft Edge Legacy settings, see Windows 10 roaming settings.) Users can selectively enable/disable these attributes using Microsoft Edge settings. Given the difference in attributes between the two versions (for example, history), users might be asked to give sync consent again.

> **NOTE**
> Unlike Microsoft Edge Legacy, Microsoft Edge doesn't use Windows credential Manager for passwords and as a result, won't sync passwords with Internet Explorer or other apps that use Windows Credential manager.

Terms of service

Terms of service for Microsoft Edge sync fall under the Microsoft software license viewable in Microsoft Edge at *edge://terms*.

See also

- Microsoft Edge Enterprise landing page
- Microsoft Edge Sync

Plan your kiosk mode transition

11/1/2022 • 4 minutes to read • Edit Online

This article provides guidance on how to transition your kiosk from Microsoft Edge Legacy to Microsoft Edge.

> **NOTE**
> This article applies to Microsoft Edge Stable, Beta and Dev Channels, version 87 or later.

> **IMPORTANT**
> When support ends for Microsoft Edge Legacy on March 9, 2021, it will be removed and replaced with Microsoft Edge on Chromium as part of the Windows Update in April. For details, go to this blog post. To continue to use your browser-based kiosk scenarios, you need to install Microsoft Edge on Chromium and set up kiosk mode prior to April's Windows Update release to your device.

Kiosk setup steps

Use the following steps as a guide to set up a kiosk in Microsoft Edge.

Step 1: Evaluate your needs against released (and upcoming) kiosk mode functionality. The following table lists the features supported by kiosk mode in Microsoft Edge on Chromium and Microsoft Edge Legacy. Use this table as a guide to transitioning to Microsoft Edge by comparing how these features are supported in both releases of Microsoft Edge.

FEATURE	DIGITAL\INTERACTIVE SIGNAGE	PUBLIC BROWSING	AVAILABLE WITH MICROSOFT EDGE VERSION (AND HIGHER)	AVAILABLE WITH MICROSOFT EDGE LEGACY
InPrivate Navigation	Y	Y	89	Y
Reset on inactivity	Y	Y	89	Y
Read only address bar (policy)	N	Y	89	N
Delete downloads on exit (policy)	Y	Y	89	N
F11 blocked (enter/exit full-screen)	Y	Y	89	Y
F12 blocked (launch Developer Tools)	Y	Y	89	Y
Multi tab support	N	Y	89	Y

FEATURE	DIGITAL\INTERACTIVE SIGNAGE	PUBLIC BROWSING	AVAILABLE WITH MICROSOFT EDGE VERSION (AND HIGHER)	AVAILABLE WITH MICROSOFT EDGE LEGACY
Allow URL support (policy)	Y	Y	89	N
Block URL support (policy)	Y	Y	89	N
Show home button (policy)	N	Y	89	Y
Manage favorites (policy)	N	Y	89	Y
Enable printer (policy)	Y	Y	89	Y
Configure the new tab page URL (policy)	N	Y	89	Y
End session button	N	Y	89	Y
All internal Microsoft Edge URLs are blocked, except for *edge://downloads* and *edge://print*	N	Y	89	Y
CTRL+N blocked (open a new window)	Y	Y	89	Y
CTRL+T blocked (open new tab)	Y	Y	89	Y
Settings and more (...) will display only the required options	Y	Y	89	Y
Restrict the launch of other applications from the browser	Y	Y	90	Y
UI print settings lockdown	Y	Y	90	Y
Set the new tab page as the home page (policy)	N	Y	90	Y

NOTE

For information about the Microsoft Edge release schedule, see Microsoft Edge release schedule.

Step2: Test the new kiosk in Microsoft Edge. We recommend that you test setting up kiosk mode in

Microsoft Edge. A quick and easy way to test kiosk mode is to configure an assigned access single app using Windows Settings as described next.

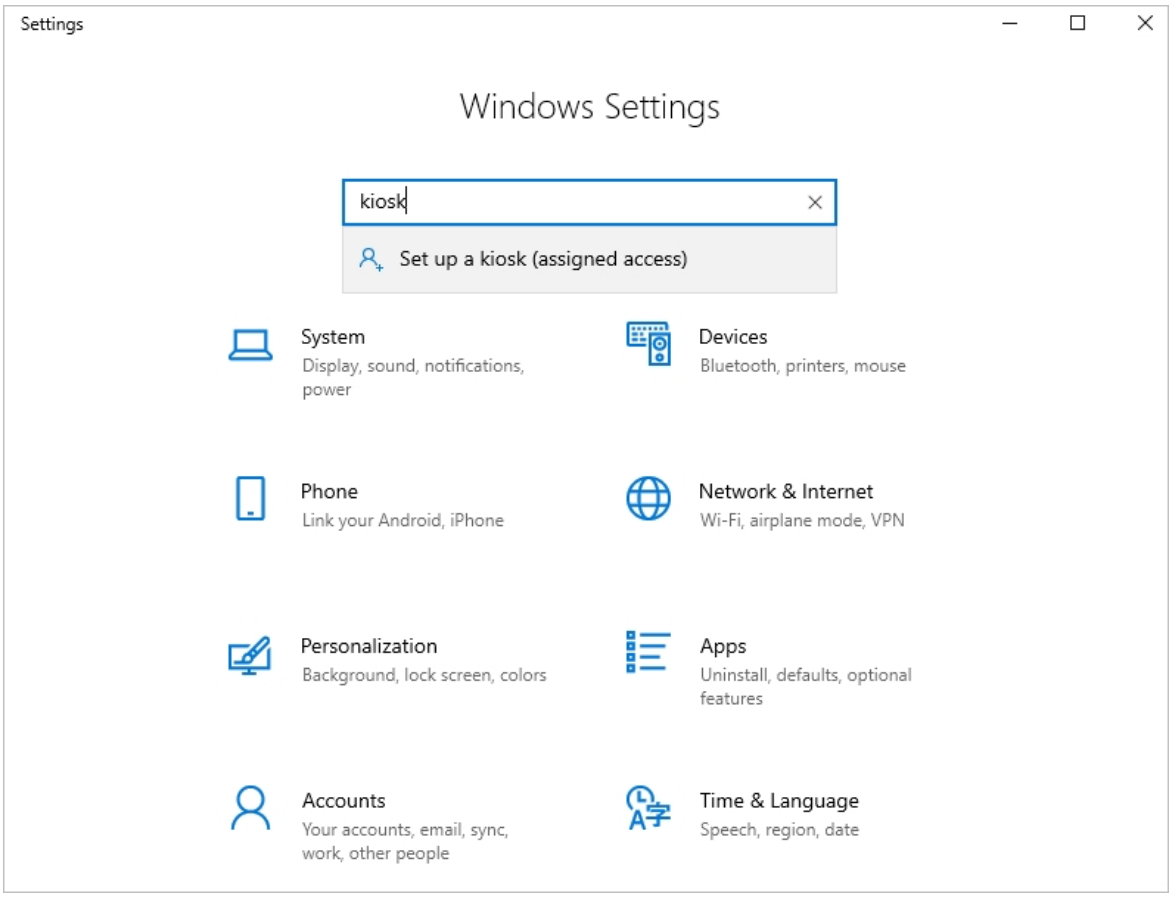
1. The minimum system updates for the operating systems listed in the next table.

OPERATING SYSTEM	VERSION	UPDATES
Windows 10	2004 or later	KB4601382 or later
Windows 10	1909	KB4601380 or later

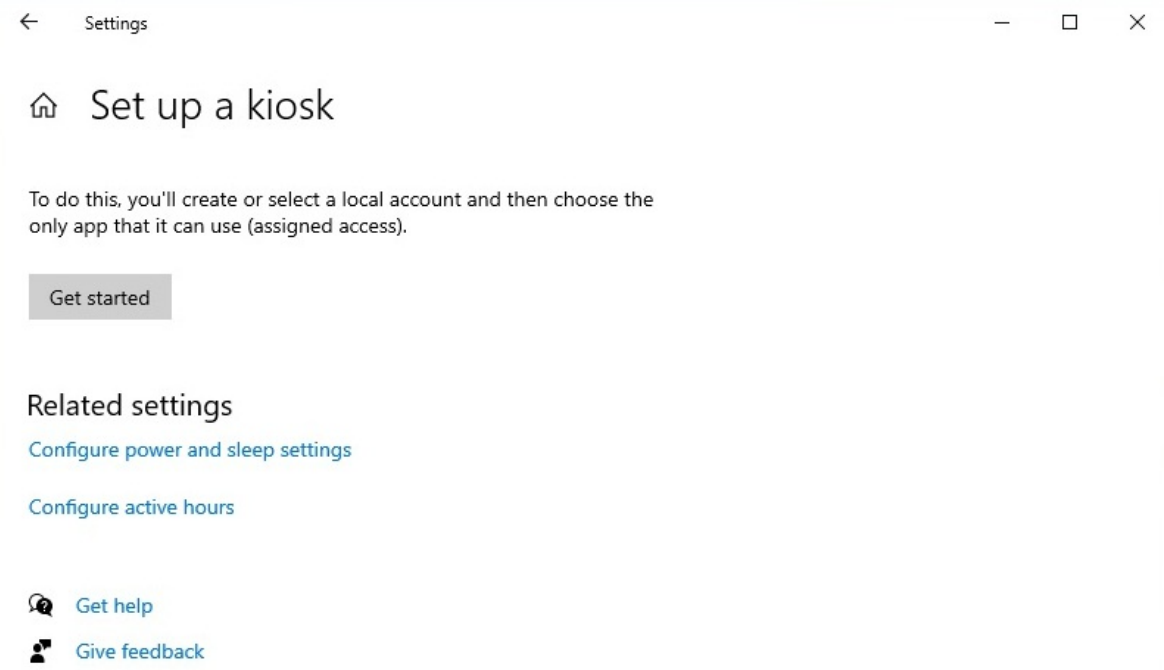
2. To test the latest features, you can download the latest Microsoft Edge Stable channel, version 89 or higher.

> **IMPORTANT**
> Because a device level installation is required, the Canary channel isn't supported.

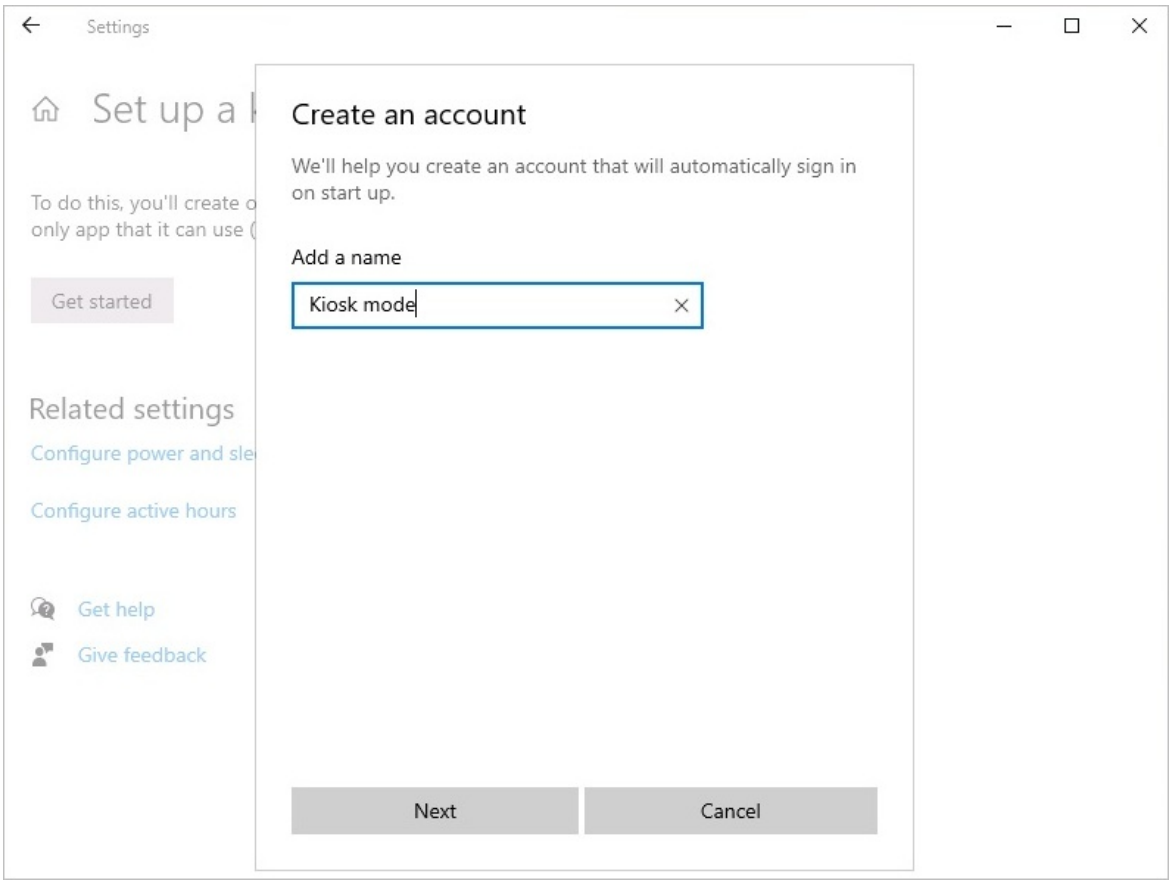
3. On the kiosk computer, open Windows Settings, and type "kiosk" in the search field. Select **Set up a kiosk (assigned access)**, shown in the next screenshot to open the dialog for creating the kiosk.



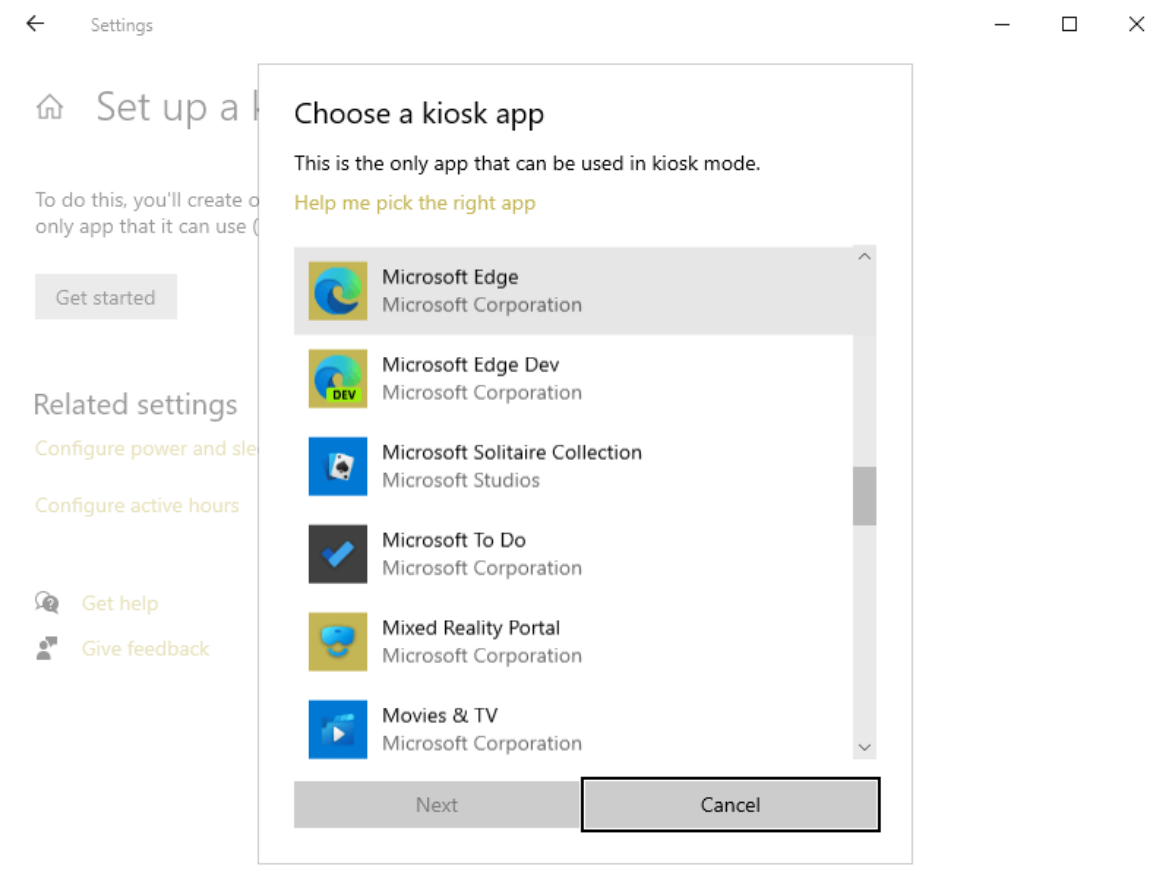
4. On the **Set up a kiosk** page, click **Get started**.


Settings
Set up a kiosk
To do this, you'll create or select a local account and then choose the only app that it can use (assigned access).
Get started
Related settings
Configure power and sleep settings
Configure active hours
Get help
Give feedback

5. Type a name to create a new kiosk account or choose an existing account from the populated dropdown list and then click**Next**.

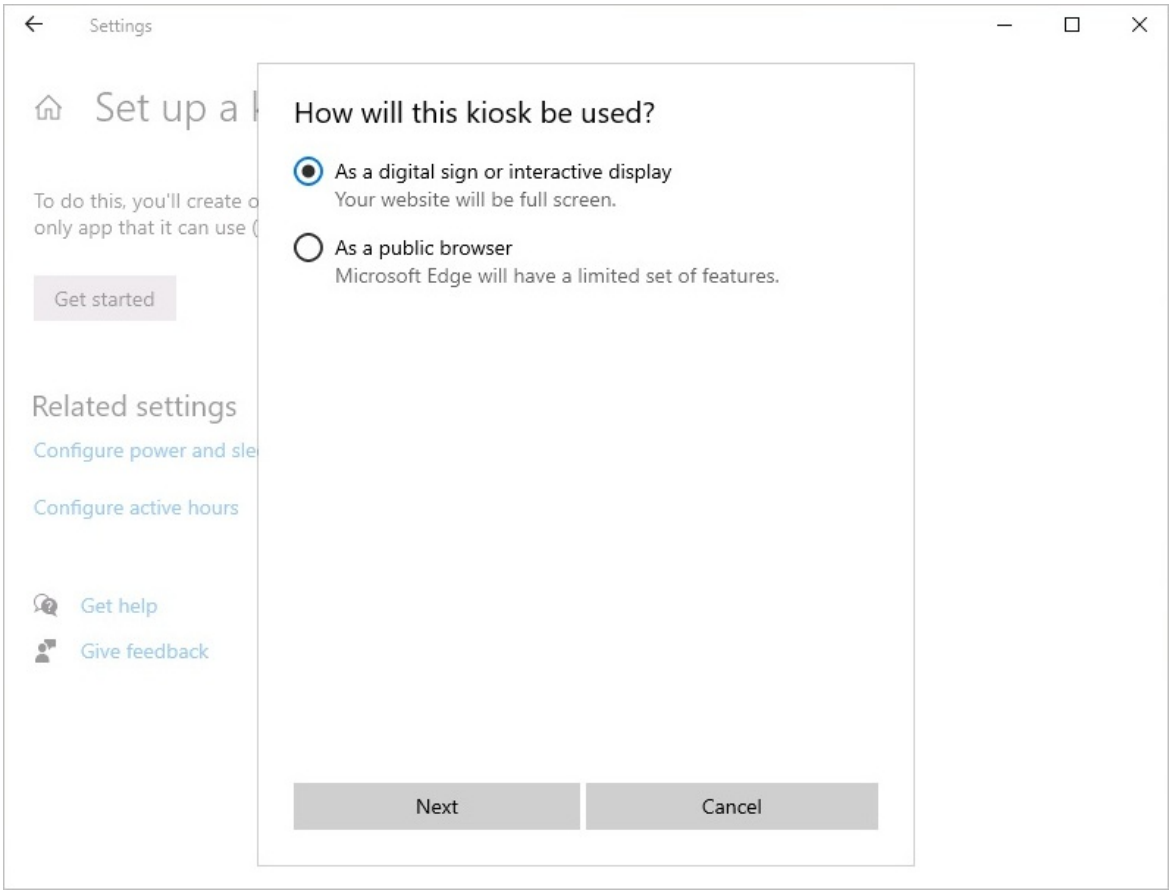


6. On the **Choose a kiosk app** page, select **Microsoft Edge** and then click **Next**.



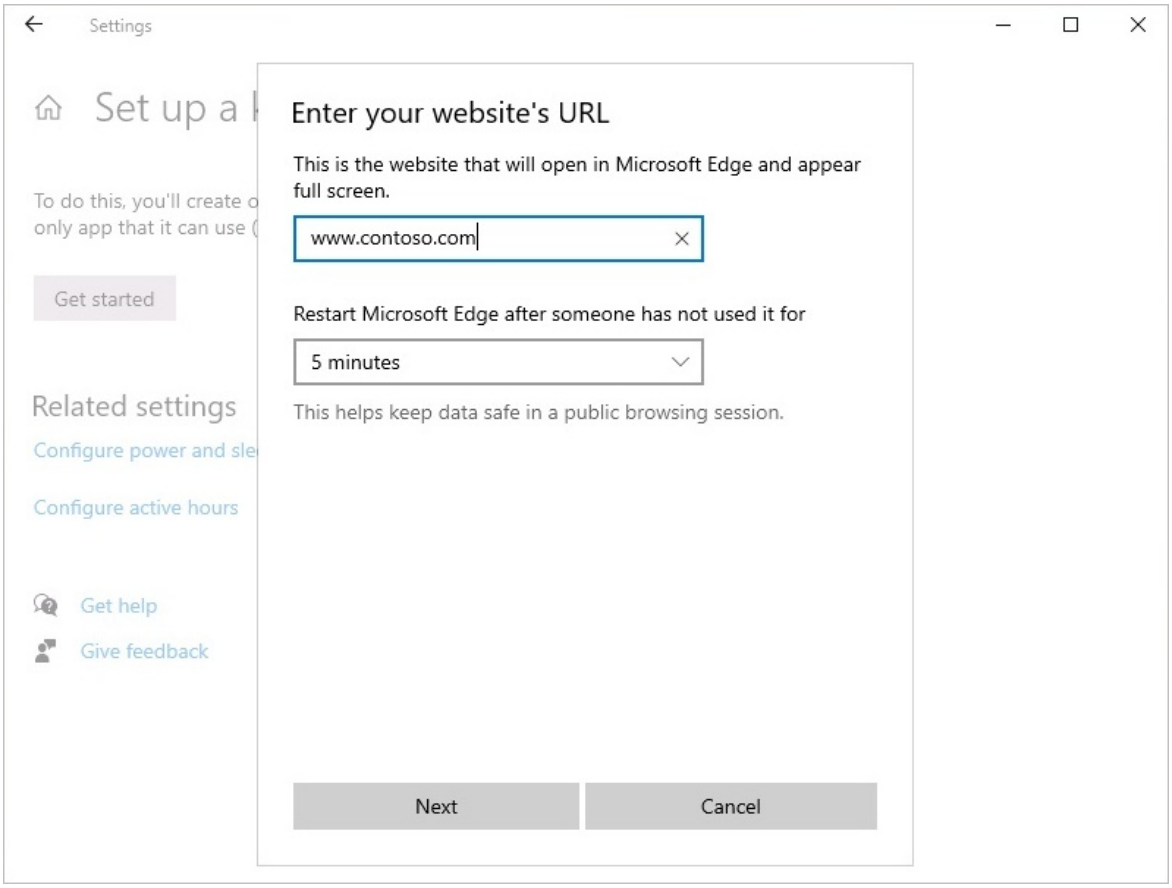
7. Select one of the following options for how Microsoft Edge displays when running in kiosk mode:

   - Digital/Interactive signage - Displays a specific site in full-screen mode, running Microsoft Edge.
   - Public browser - Runs a limited multi-tab version of Microsoft Edge.

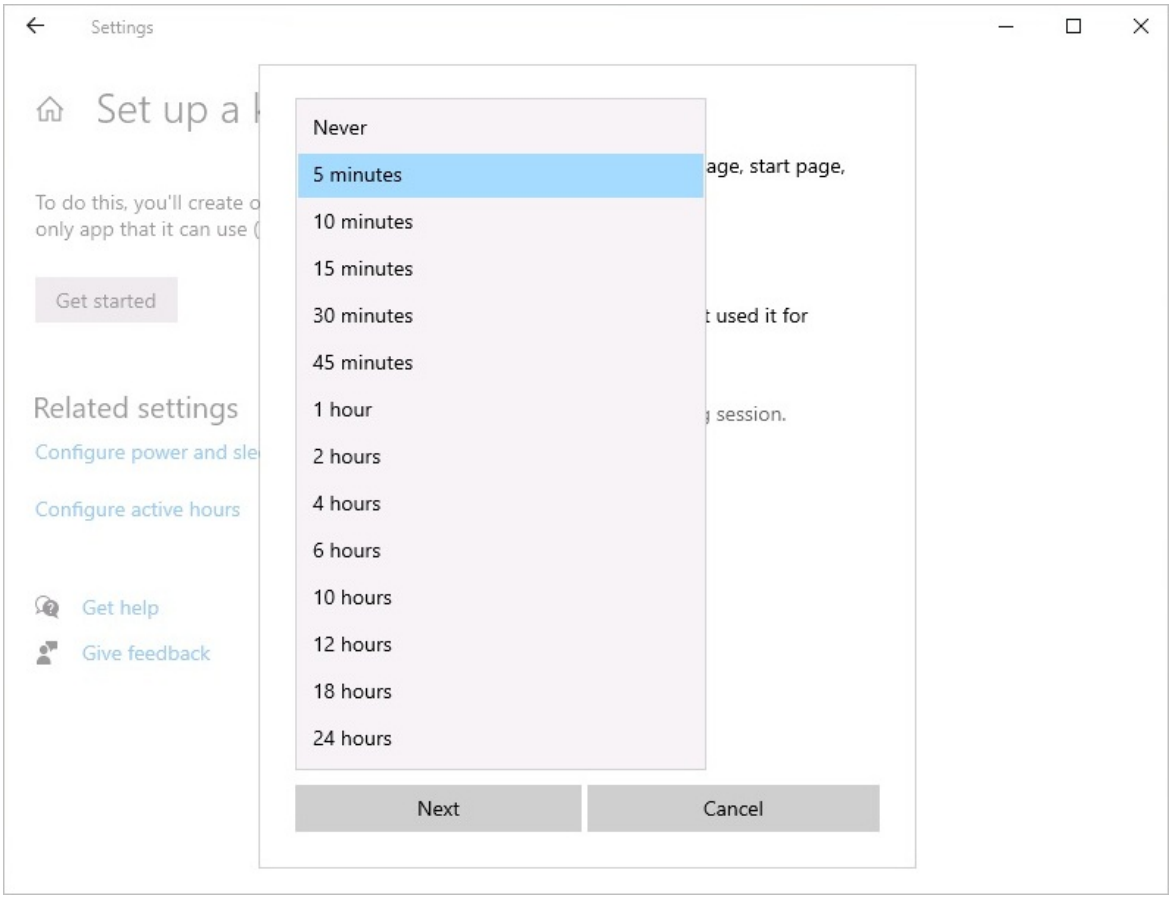


8. Select **Next**.

9. Type the URL to load when the kiosk launches.

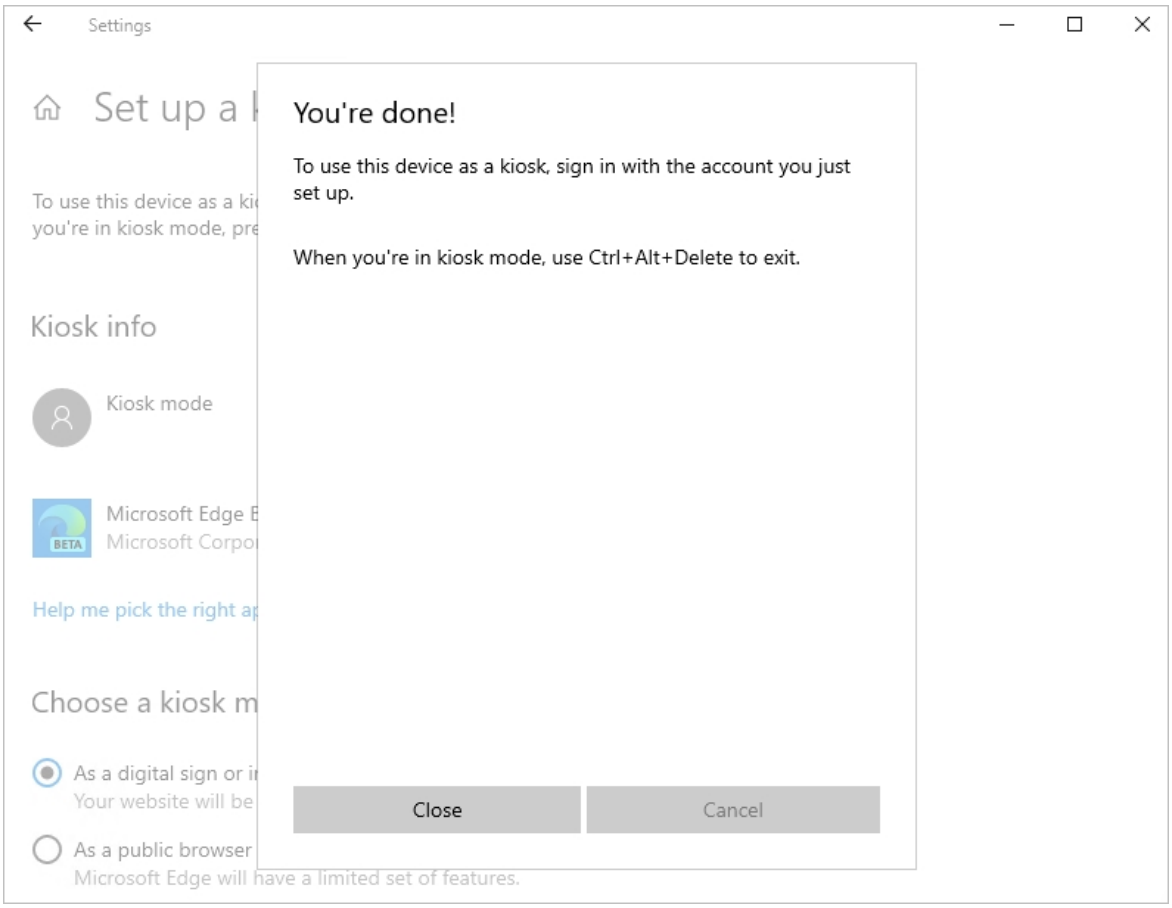

Settings
Set up a k
To do this, you'll create o
only app that it can use (
Get started
Related settings
Configure power and sle
Configure active hours
Get help
Give feedback
Enter your website's URL
This is the website that will open in Microsoft Edge and appear full screen.
www.contoso.com
Restart Microsoft Edge after someone has not used it for
5 minutes
This helps keep data safe in a public browsing session.
Next
Cancel

10. Accept the default value of5 minutesfor the idle time or provide a value of your own.



11. Click**Next**.

12. Close the**Settings**window to save and apply your choices.


Settings
Set up a
You're done!
To use this device as a kiosk, sign in with the account you just set up.
When you're in kiosk mode, use Ctrl+Alt+Delete to exit.
Kiosk info
Kiosk mode
Close
Cancel

13. Sign out from the kiosk device and sign in with the local kiosk account to validate the configuration.

Step 3: Develop a transition plan. Based on your testing and organizational needs, we recommend developing a transition plan and moving to Microsoft Edge on Chromium before support ends for Microsoft Edge Legacy on March 9, 2021.

Additional scenarios that require you to recreate an existing kiosk mode

If you update to Windows 10, version 20H2, Microsoft Edge on Chromium will be installed, and Microsoft Edge Legacy will be hidden. In this instance, you will need to set up kiosk mode again in Microsoft Edge on Chromium.

How to get help

Kiosk mode may be an important part of your everyday business, so we want to help make this transition as smooth as possible and help you avoid disruptions. If your business needs help transitioning to Microsoft Edge on Chromium:

- Support is available from Microsoft.
- FastTrack support is also available at no additional charge to customers with 150 or more paid seats of Windows 10 Enterprise.
- App Assure is available if you experience site or app compatibility issues.

See also

- Microsoft Edge Enterprise landing page
- New Microsoft Edge to replace Microsoft Edge Legacy with April's Windows 10 Update Tuesday release

Configure Microsoft Edge kiosk mode

11/1/2022 • 6 minutes to read • Edit Online

This article describes how to configure Microsoft Edge kiosk mode options that you can pilot. There's also a roadmap of features we're targeting.

> **NOTE**
> This article applies to Microsoft Edge version 87 or later.

> **IMPORTANT**
> Invoke Microsoft Edge kiosk mode features on Windows 10 using the command line arguments provided in Use kiosk mode features.

Overview

Microsoft Edge kiosk mode offers two lockdown experiences of the browser so organizations can create, manage, and provide the best experience for their customers. The following lockdown experiences are available:

- **Digital/Interactive Signage** experience - Displays a specific site in full-screen mode.
- **Public-Browsing** experience - Runs a limited multi-tab version of Microsoft Edge.

Both experiences are running a Microsoft Edge InPrivate session, which protects user data.

Set up Microsoft Edge kiosk mode

An initial set of kiosk mode features is available to test with Microsoft Edge Stable Channel, version 87. You can download the latest version from Microsoft Edge (Official Stable Channel).

Kiosk mode supported features

The following table lists the features supported by kiosk mode in Microsoft Edge and Microsoft Edge Legacy. Use this table as a guide to transitioning to Microsoft Edge by comparing how these features are supported in both versions of Microsoft Edge.

FEATURE	DIGITAL\INTERACTIVE SIGNAGE	PUBLIC BROWSING	AVAILABLE WITH MICROSOFT EDGE VERSION (AND HIGHER)	AVAILABLE WITH MICROSOFT EDGE LEGACY
InPrivate Navigation	Y	Y	89	Y
Reset on inactivity	Y	Y	89	Y
Read only address bar (policy)	N	Y	89	N
Delete downloads on exit (policy)	Y	Y	89	N

FEATURE	DIGITAL\INTERACTIVE SIGNAGE	PUBLIC BROWSING	AVAILABLE WITH MICROSOFT EDGE VERSION (AND HIGHER)	AVAILABLE WITH MICROSOFT EDGE LEGACY
F11 blocked (enter/exit full-screen)	Y	Y	89	Y
F12 blocked (launch Developer Tools)	Y	Y	89	Y
Multi tab support	N	Y	89	Y
Allow URL support (policy)	Y	Y	89	N
Block URL support (policy)	Y	Y	89	N
Show home button (policy)	N	Y	89	Y
Manage favorites (policy)	N	Y	89	Y
Enable printer (policy)	Y	Y	89	Y
Configure the new tab page URL (policy)	N	Y	89	Y
End session button *	N	Y	89	Y
All internal Microsoft Edge URLs are blocked, except for *edge://downloads* and *edge://print*	N	Y	89	Y
CTRL+N blocked (open a new window) *	Y	Y	89	Y
CTRL+T blocked (open new tab)	Y	N	89	Y
Settings and more (...) will display only the required options	Y	Y	89	Y
Restrict the launch of other applications from the browser	Y	Y	90	Y
UI print settings lockdown	Y	Y	90	Y

FEATURE	DIGITAL\INTERACTIVE SIGNAGE	PUBLIC BROWSING	AVAILABLE WITH MICROSOFT EDGE VERSION (AND HIGHER)	AVAILABLE WITH MICROSOFT EDGE LEGACY
Set the new tab page as the home page (policy)	N	Y	90	Y

> **NOTE**
> Features followed by "*" are only enabled in an assigned access single app scenario.

Use kiosk mode features

Microsoft Edge kiosk mode features can be invoked with the following Windows 10 command-line options for Digital/Interactive signage and Public browsing.

Kiosk mode Digital/Interactive signage

```
msedge.exe --kiosk www.contoso.com --edge-kiosk-type=fullscreen
```

Kiosk mode Public browsing

```
msedge.exe --kiosk www.contoso.com --edge-kiosk-type=public-browsing
```

Kiosk mode Download Files on Exit

To set up Microsoft Edge to remove downloaded files when a Kiosk instance is closed, the following two Group Policies must be configured:

- Delete downloads on exit = Enabled
- Set download directory = ${local_app_data}\Microsoft\Edge\KioskDownloads

Additional command-line options

- **--no-first-run**: Disable the first Microsoft Edge run experience.

  ```
  msedge.exe --kiosk www.contoso.com --edge-kiosk-type=fullscreen --no-first-run
  ```

  ```
  msedge.exe --kiosk www.contoso.com --edge-kiosk-type=public-browsing --no-first-run
  ```

- **--kiosk-idle-timeout-minutes=**: Change the time (in minutes) from the last user activity before Microsoft Edge kiosk mode resets the user's session by closing the browser. Note: this flag will not restart Microsoft Edge after it's closed. A separate technology, such as Assigned Access or Shell Launch is required to automatically restart Edge after the idle timeout. Replace "value" in the next example with the number of minutes.

  ```
  --kiosk-idle-timeout-minutes=value
  ```

  The following "values" are supported:

  - Default values (in minutes)
    - Full screen - 0 (turned off)

    - Public browsing - 5 minutes
- Allowed values
    - 0 - turns off the timer
    - 1-1440 minutes for reset on idle timer

```
msedge.exe --kiosk www.contoso.com --edge-kiosk-type=fullscreen --kiosk-idle-timeout-minutes=1
```

```
msedge.exe --kiosk www.contoso.com --edge-kiosk-type=public-browsing --kiosk-idle-timeout-minutes=1
```

Support policies for kiosk mode

Use any of the Microsoft Edge policies listed in the following table to enhance the kiosk experience for the Microsoft Edge kiosk mode type you configure. To learn more about these policies, see Microsoft Edge – Browser policy reference.

> **NOTE**
> Policy configuration isn't limited to the policies listed in the following table, however additional policies should be tested to ensure that kiosk mode functionality isn't negatively affected.

GROUP POLICY	DIGITAL\INTERACTIVE SIGNAGE	PUBLIC BROWSING SINGLE-APP
Printing	Y	Y
HomePageLocation	N	Y
ShowHomeButton	N	Y
NewTabPageLocation	N	Y
FavoritesBarEnabled	N	Y
URLAllowlist	Y	Y
URLBlocklist	Y	Y
ManagedSearchEngines	N	Y
UserFeedbackAllowed	N	Y
VerticalTabsAllowed	N	Y
SmartScreen settings	Y	Y
EdgeCollectionsEnabled	Y	Y

Microsoft Edge with assigned access

Single app kiosk

Microsoft Edge version 90 kiosk mode offers an extensive list of features. See the section of Kiosk mode supported features. With the following Windows updates you can configure Microsoft Edge via assigned access single app.

OPERATING SYSTEM	VERSION	UPDATES
Windows 10	2004 or later	KB4601382 or later
Windows 10	1909	KB4601380 or later

You can manage Microsoft Edge kiosk mode assigned access single app via Windows Settings and Intune.

Multi-app kiosk

Microsoft Edge can be run with multi-app assigned access on Windows 10, which is the equivalent of Microsoft Edge Legacy "Normal browsing" kiosk mode type. To configure Microsoft Edge with multi-app assigned access, follow the instructions on how to Set up a multi-app kiosk. (The AUMID for the Microsoft Edge Stable channel is **Microsoft.MicrosoftEdge.Stable_8wekyb3d8bbwe!MSEDGE**).

When using Microsoft Edge with multi-app assigned access, you can configure Microsoft Edge kiosk to use the Microsoft Edge browser policies to configure the browsing experience to meet your unique requirements.

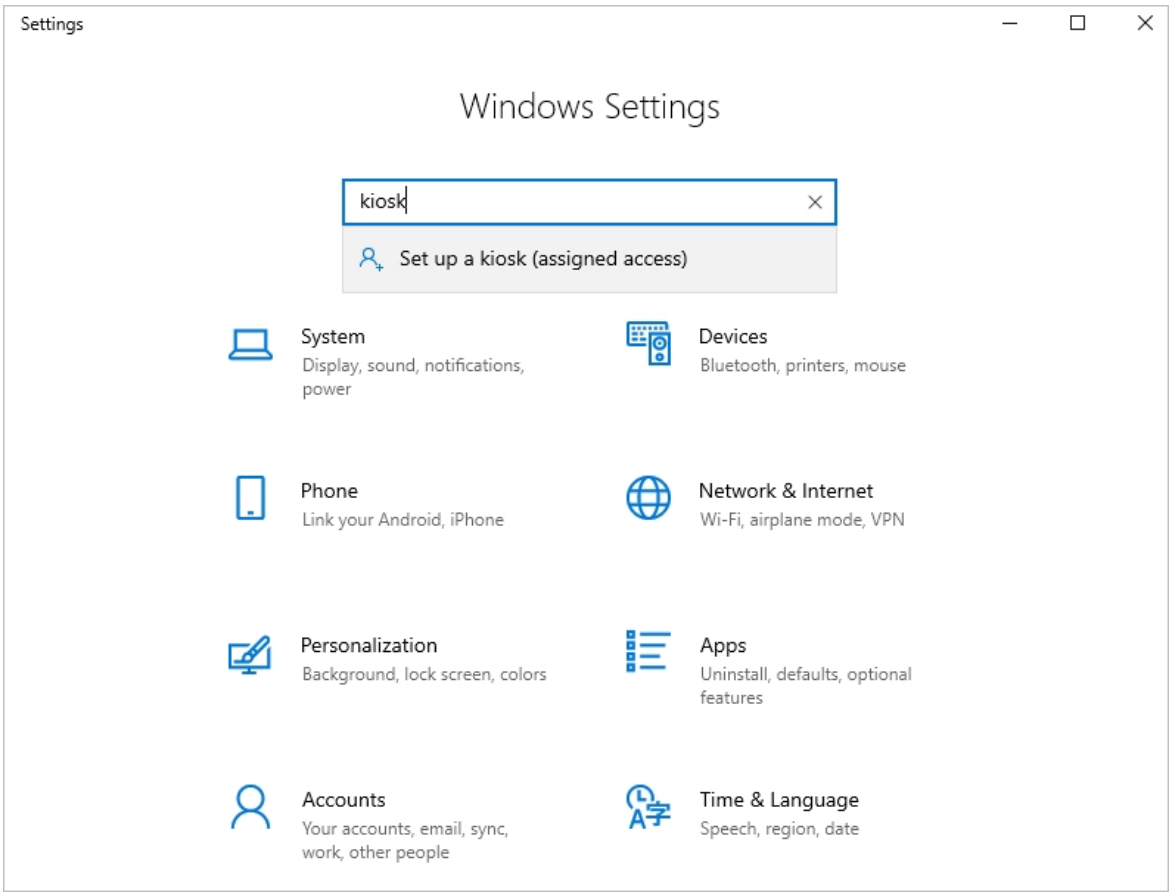
Configure using Windows Settings

Windows Settings is the simplest way to set up one or two single-app kiosk devices. Use the following steps to set up a single-app kiosk computer.

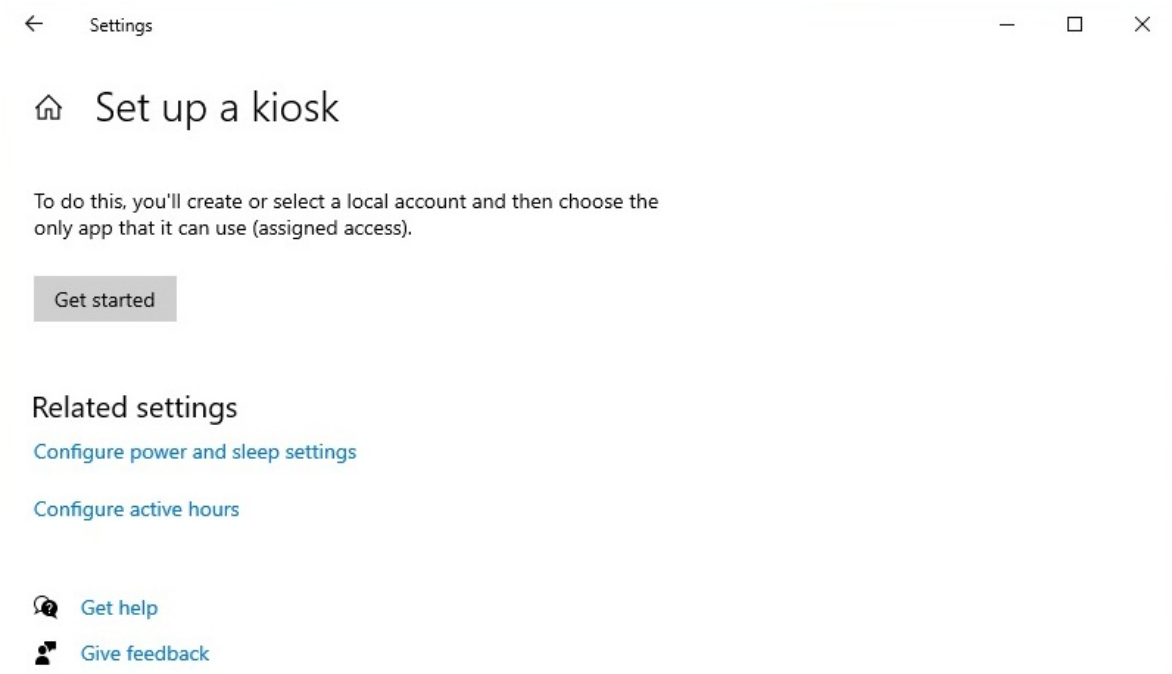
1. The minimum system updates for the operating systems listed in the next table.

OPERATING SYSTEM	VERSION	UPDATES
Windows 10	2004 or later	KB4601382 or later
Windows 10	1909	KB4601380 or later

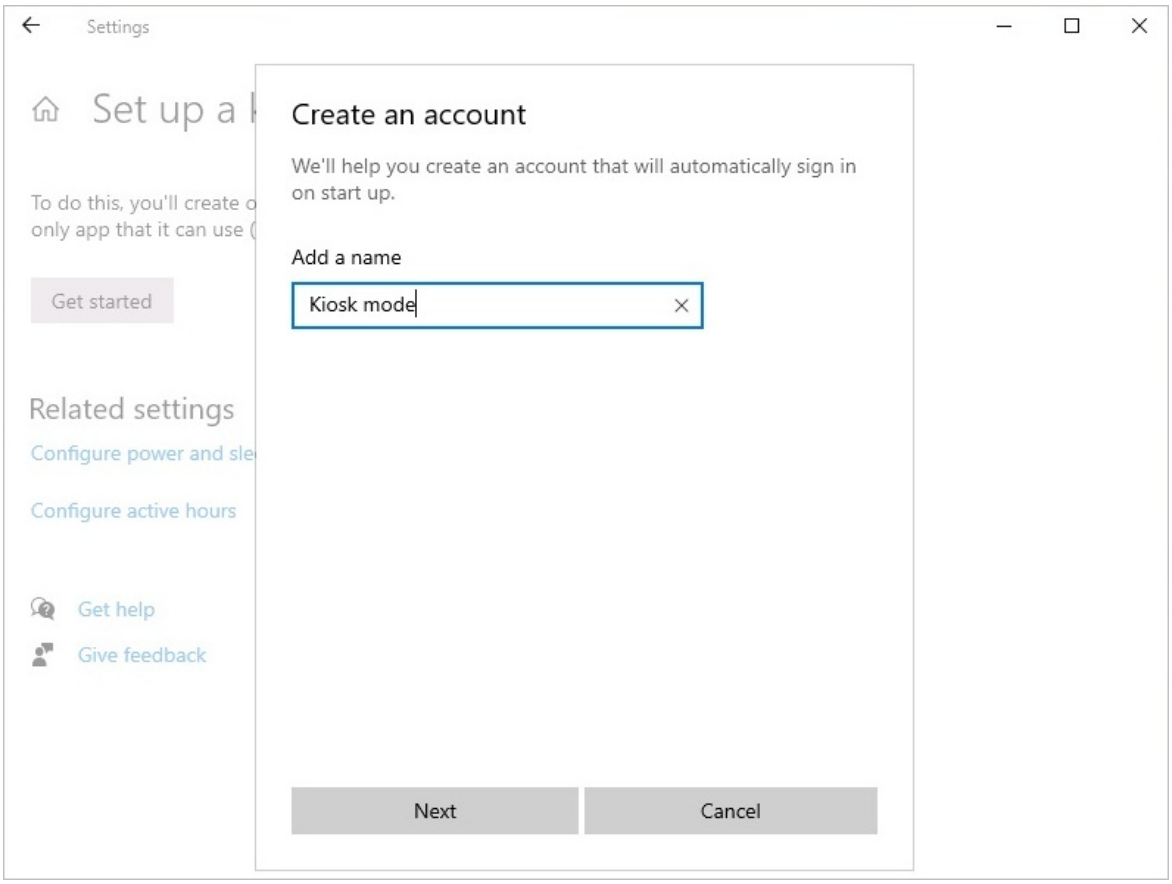
2. To test the latest features, you can download the latest Microsoft Edge Stable channel, version 89 or higher.
3. On the kiosk computer, open Windows Settings, and type "kiosk" in the search field. Select **Set up a kiosk (assigned access)**, shown in the next screenshot to open the dialog for creating the kiosk.



4. On the **Set up a kiosk** page, select **Get started**.

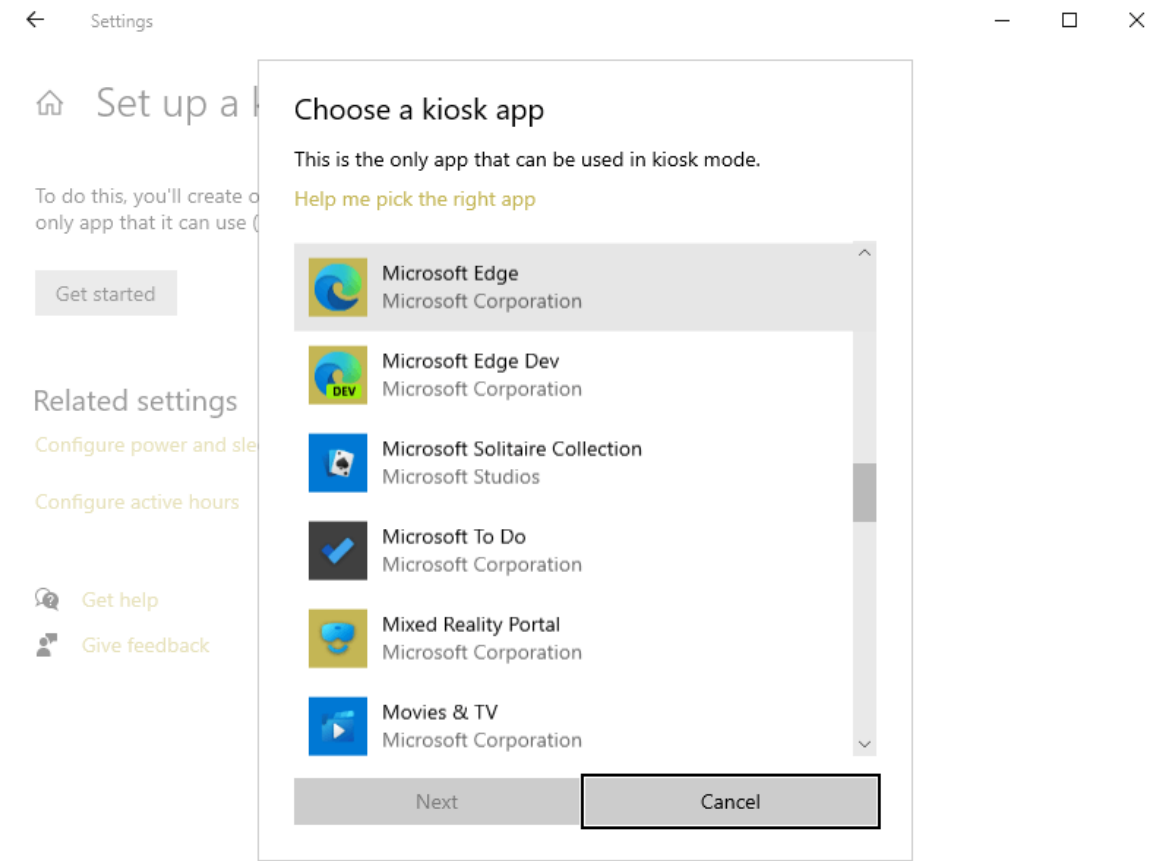

Settings
Set up a kiosk
To do this, you'll create or select a local account and then choose the only app that it can use (assigned access).
Get started
Related settings
Configure power and sleep settings
Configure active hours
Get help
Give feedback

5. Type a name to create a new kiosk account or choose an existing account from the populated dropdown list and then select **Next**.



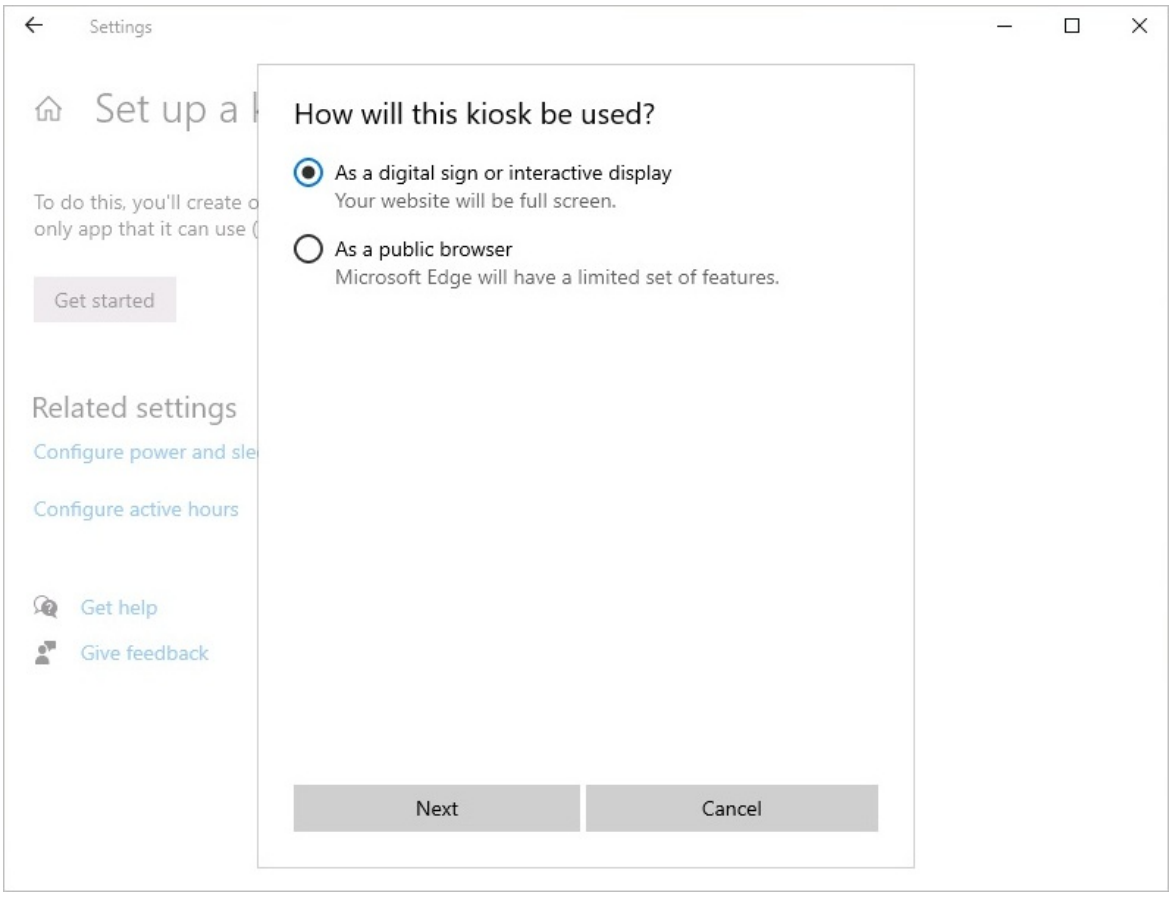
6. On the **Choose a kiosk app** page, select **Microsoft Edge**, and then select **Next**.

> **NOTE**
>
> This only applies to Microsoft Edge Dev, Beta, and Stable channels.



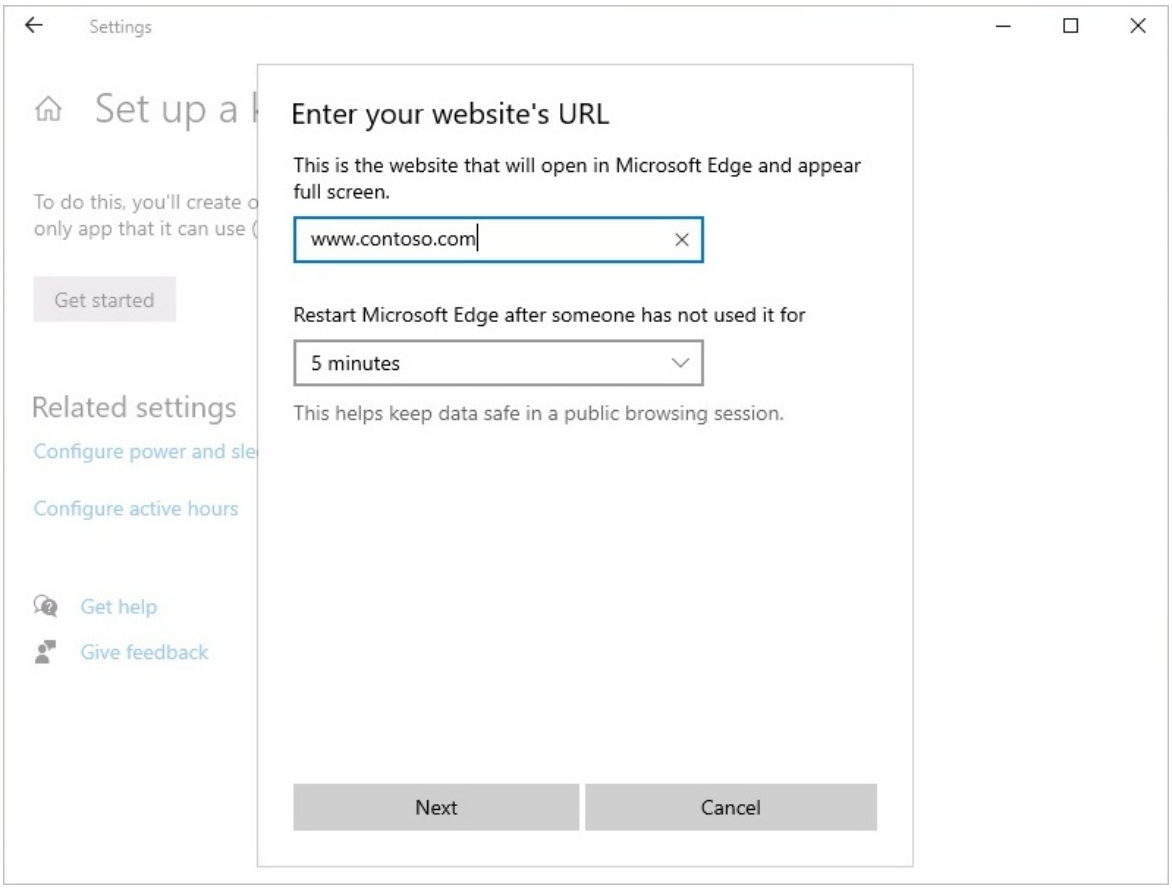
7. Pick one of the following options for how Microsoft Edge displays when running in kiosk mode:

   - Digital/Interactive signage - Displays a specific site in full-screen mode, running Microsoft Edge.
   - Public browser - Runs a limited multi-tab version of Microsoft Edge.

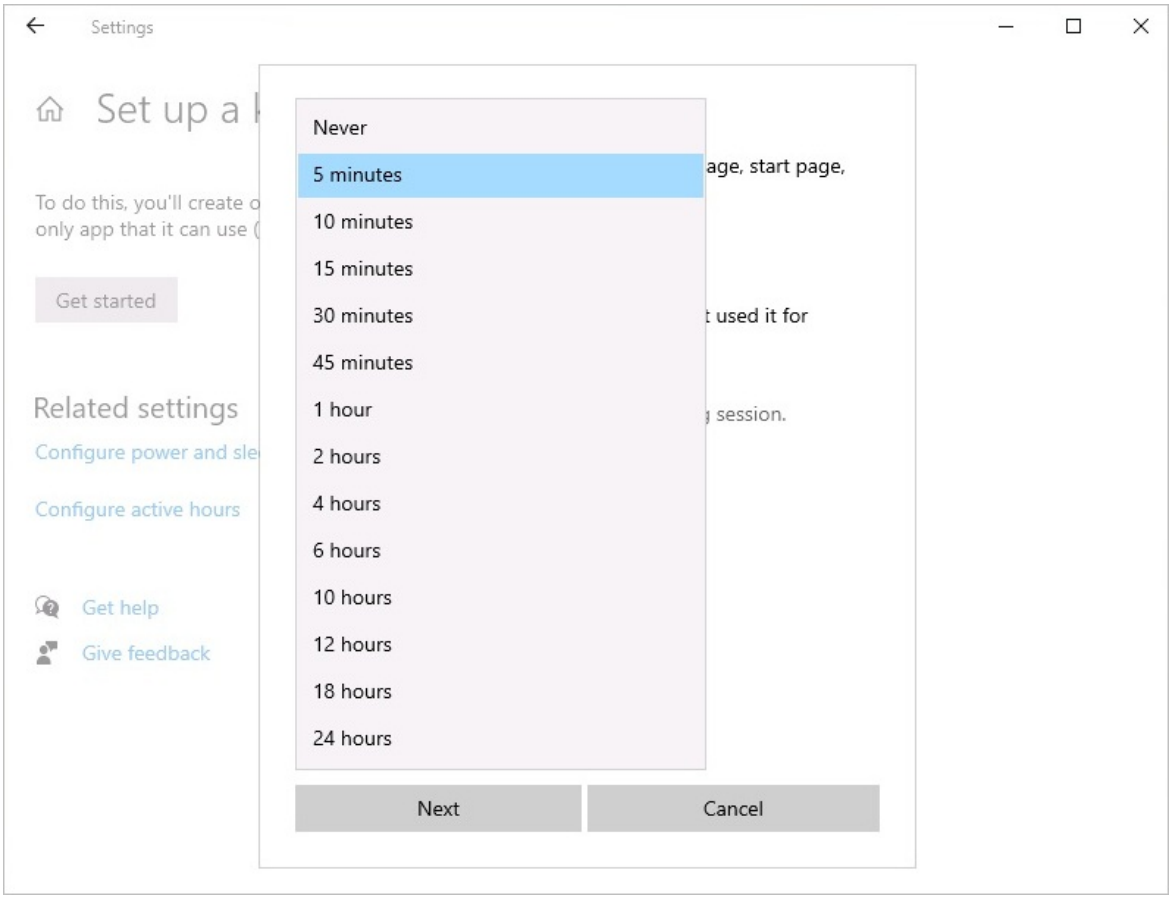


8. Select **Next**.

9. Type the URL to load when the kiosk launches.

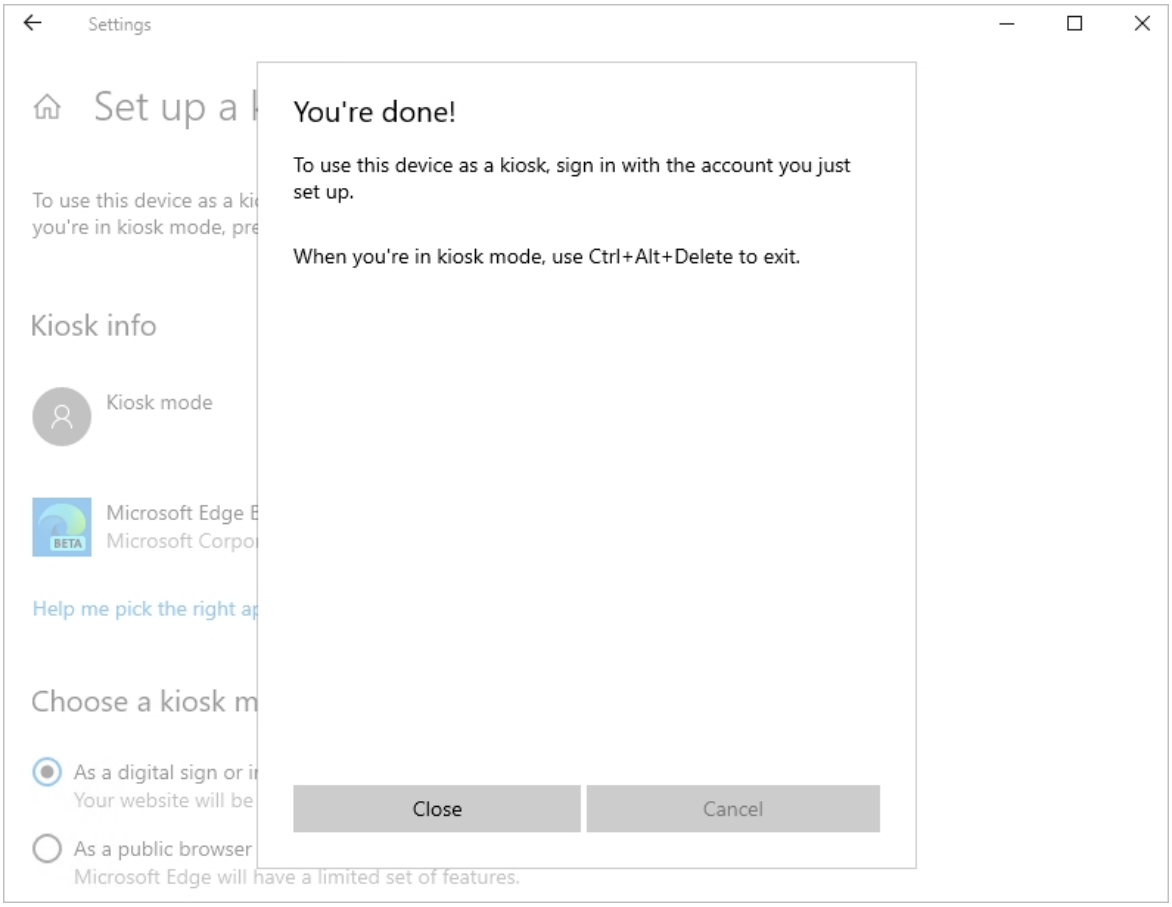

Settings
Set up a
Enter your website's URL
This is the website that will open in Microsoft Edge and appear full screen.
www.contoso.com
Restart Microsoft Edge after someone has not used it for
5 minutes
This helps keep data safe in a public browsing session.
Next
Cancel
To do this, you'll create o
only app that it can use (
Get started
Related settings
Configure power and sle
Configure active hours
Get help
Give feedback

10. Accept the default value of5 minutesfor the idle time or provide a value of your own.



11. Select**Next**.

12. Close the**Settings**window to save and apply your choices.


Settings
Set up a k
To use this device as a ki
you're in kiosk mode, pre
Kiosk info
Kiosk mode
Microsoft Edge E
Microsoft Corpo
BETA
Help me pick the right ap
Choose a kiosk m
As a digital sign or i
Your website will be
As a public browser
Microsoft Edge will have a limited set of features.
You're done!
To use this device as a kiosk, sign in with the account you just set up.
When you're in kiosk mode, use Ctrl+Alt+Delete to exit.
Close
Cancel

13. Sign out from the kiosk device and sign in with the local kiosk account to validate the configuration.

Functional limitations

With the release of this preview version of kiosk mode we're continuing work on improving the product and adding new features.

We currently don't support the following features and recommend that you turn off:

- InPrivateModeAvailability
- IsolateOrigins
- ManagedFavorites
- EdgeShoppingAssistantEnabled
- EdgeCollectionsEnabled
- UserFeedbackAllowed
- DefaultPopupsSetting
- StartupBoostEnabled
- Extensions
- BackgroundModeEnabled
- UserFeedbackAllowed

See also

- Microsoft Edge Enterprise landing page
- Plan your deployment of Microsoft Edge
- Configure kiosks and digital signs on Windows desktop editions
- Plan your kiosk mode transition

Manage Microsoft Edge extensions in the enterprise

11/1/2022 • 6 minutes to read • Edit Online

This article provides best practice guidance for admins who are managing Microsoft Edge extensions in their organizations. You can use the information in this article to develop a strategy for managing extensions in your organization.

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

Introduction

Organizations want to protect corporate and user data and evaluate browser extensions to ensure that they're safe and relevant to their enterprise. Admins want to:

- Prevent bad apps and extensions from being installed.
- Keep extensions that users need to do their job.
- Manage access to user and company data.

This article is the first in a series that that helps admins manage extensions to provide a safe and productive experience for their users. This series walks through the different options and helps you pick the best method for managing extensions. The series consists of the following articles:

- Manage Microsoft Edge extensions in the enterprise. Create a strategy to manage extensions and set up administrative templates required for managing the browser.
- Use group policies to manage Microsoft Edge extensions. Options using group policies to manage extensions.
- Create a web store to host Microsoft Edge extensions. Create and host extensions.
- FAQ for Microsoft Edge Extensions. Frequently Asked Questions.

Things to consider when managing extensions

Your users need access to certain apps, sites, and extensions to do their jobs while at the same time protecting users and company data. An effective security strategy involves asking the right questions for your enterprise and how extensions can fit your company's needs. Some of the key questions to ask are:

- What regulations and compliance measures do I need to adhere to?
- Do some extensions ask for overly broad permissions, which could go against my company's data security policies?
- How much user or corporate data is stored on my users' devices?

As you answer these questions, you can use the granular policies that Microsoft Edge provides to:

- Block or allow extensions on users' computers based on your data protection policies.
- Force-install extensions on your users' devices so they have tools that they need to be productive.
- Allowlist or blocklist extensions to allow the least amount of rights needed for your users to do their work.

The traditional model for managing extensions uses the allowlist and blocklist approach for specific extensions. However, Microsoft Edge also lets you manage the permissions requested by extensions. Using this model, you

can decide which rights and permissions you want to allow extensions to use on your computers and devices, and then implement a global policy that allows or block extensions based on your requirements.

Understand extension permissions

Extensions can require rights to make changes on a device or a web page to run properly. These rights are called permissions. Developers must list what rights and access their extensions need. There are two main categories for permissions, and many extensions need both of the following permissions:

- Host permissions require the extension to list webpages it may view or modify.
- Device permissions are the rights needed by an extension on the device where it's running.

Some examples of these permissions are: access to a USB port, storage or viewing screen, and communicating with native programs.

Get ready to manage extensions

Before you begin

The extensions options assume that you already have Microsoft Edge managed for your users. For more information about setting up administrative templates for Microsoft Edge policies, see:

- Configure Microsoft Edge policy settings on Windows
- Configure for Windows with Intune
- Configure for Windows with Mobile Device Management
- Configure for macOS using a .plist
- Configure for macOS with Jamf

The configuration steps in this article are for Windows, for the corresponding implementation in MAC/Linux, see the Microsoft Edge browser policy reference.

Decide which extensions to allow

Most organizations should manage extensions by their permissions and what websites they have access to. This method is more secure, easier to manage, and is scalable for large organizations.

- Blocked/allowed permissions – Lets you control extensions by the permissions they need.
- Runtime block hosts – Lets you to control what websites these extensions can access.

Using this approach saves time because you only need to set these once. And with the run-time hosts policy, your most important sites will be protected.There are other options as well such as:

- Force install extensions – Lets you install extensions silently.
- Allowlist/blocklist (if required) – Decide what extensions are allowed to be installed.

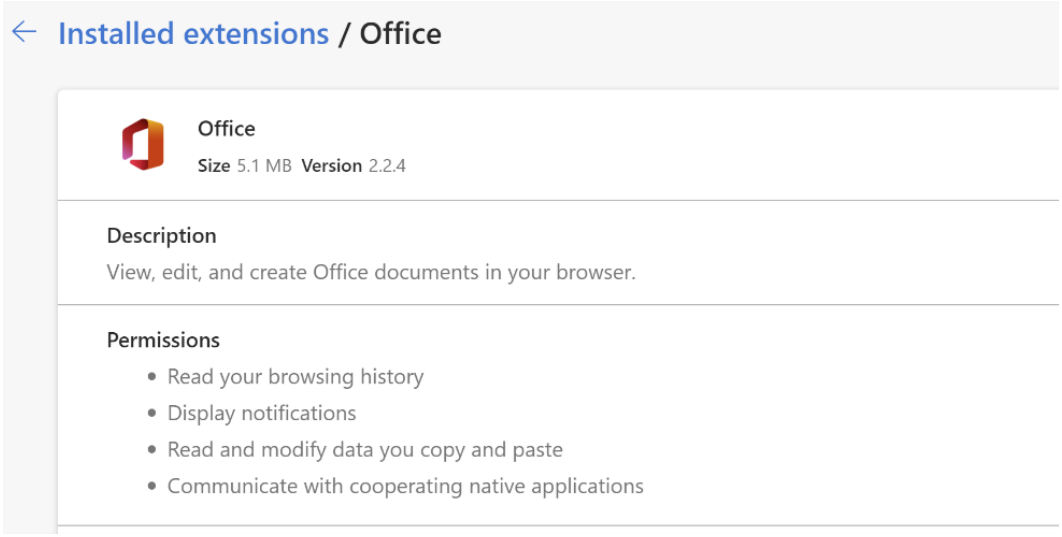
Use the following steps as a guide to decide which extensions to allow in your organization.

1. Create a list of which extensions employees need on their computers. Test the extensions in a test environment to diagnose any compatibility issues with internal apps.
2. Choose which sites need to be more secure.
    - Find out which sensitive internal websites or domains you need to block extensions from making changes to or reading data from.
    - Prevent access to these sites by blocking the API calls when the extension is run. This includes blocking web requests, reading cookies, JavaScript injection, XHR, and so on.

3. Determine which permissions are required for these extensions to run. Identify which permissions pose potential risks to your users.

   - Audit the extensions your users have installed and see what permissions they need. You can look at the web app manifest JSON file in the code of the extension. Take the following steps to see what rights the extension needs:

     - Install the extension from the Microsoft Edge Add-ons website or the Chrome Web Store.
     - Test the extension and understand how it works in your organization.
     - Review the permissions that the extension requires by navigating to *edge://extensions*. For example, the Microsoft Office extension shown in the next screenshot requests the permissions "Read your browsing history" and "Display notifications". Weigh the usefulness of this extension against the level of permissions it requests. After you approve an extension for your organization, manage it using the following tools.


Installed extensions / Office
Office
Size 5.1 MB Version 2.2.4
Description
View, edit, and create Office documents in your browser.
Permissions
Read your browsing history
Display notifications
Read and modify data you copy and paste
Communicate with cooperating native applications

   - You can also validate the extensions requested by users in your organization before approving them in the organization. Some of the permissions that extensions use can be vague. For business-critical apps, you can reach out to the app developer or vendor directly to get more information about the extension or look at the source code. They should be able to detail the changes that the extension can make on devices and websites.

   - Review the Declare Permissions list, which lists all permissions an extension can use. From this list, you can decide which permissions you want to allow in your organization.

4. Create a master list from the data you collected.This list will include the following information:

   - **Required extensions**. This list could be organized by department, office location, or other relevant information.
   - **Extension Allowlist**. Required extensions with permissions that may be blocked but will be allowed to run. These extensions are needed by your users or are determined to not be a risk through conversations with the vendor.
   - **Extension Blocklist**. Extensions that are blocked from installation. The extensions in this list have the permissions that aren't allowed to run. Also include the core sites and domains to be kept secure and not allowed extension access. Later you can compare this blocklist to others you already have in place. You might find that you can relax your current blocklist policies.

5. Present your list to your stakeholders and the IT team to get buy in.

6. Test out the new policy in your lab or with a small pilot in your organization.

7. Roll out these new sets of policies to employees in phases. For more information, see Use group policies to manage Microsoft Edge extensions.

8. Review feedback from your users.

9. Repeat and fine-tune the process monthly, quarterly, or yearly.

With your baseline of allowed permissions enforced and sensitive corporate sites protected, you can provide your enterprise with more security while providing a better experience for users. Staff might install extensions that they couldn't before, but not run them on sensitive business sites.

See also

- Use group policies to manage Microsoft Edge extensions
- Create a web store to host Microsoft Edge extensions
- Reference guide for the ExtensionSettings policy
- FAQ for Microsoft Edge Extensions
- Microsoft Edge Enterprise landing page

Manage the sidebar in Microsoft Edge

11/1/2022 • 2 minutes to read • Edit Online

This article describes the sidebar in Microsoft Edge and provides information about the procedures that admins can use to manage this feature in their organization.

Introduction to the sidebar

For a growing number of people, the browser has become the place where work happens. As the transition from juggling apps to switching tabs entrenches web-based tools in our workflows, the risks to productivity mount. With the sidebar in Microsoft Edge, Enterprise users can access the productivity tools they need while staying in their workflow.

Use group policies to manage the sidebar

Admins have several policy options for deploying and managing the sidebar in their organization. The following policies can be applied to the sidebar and the individual apps referenced by the sidebar.

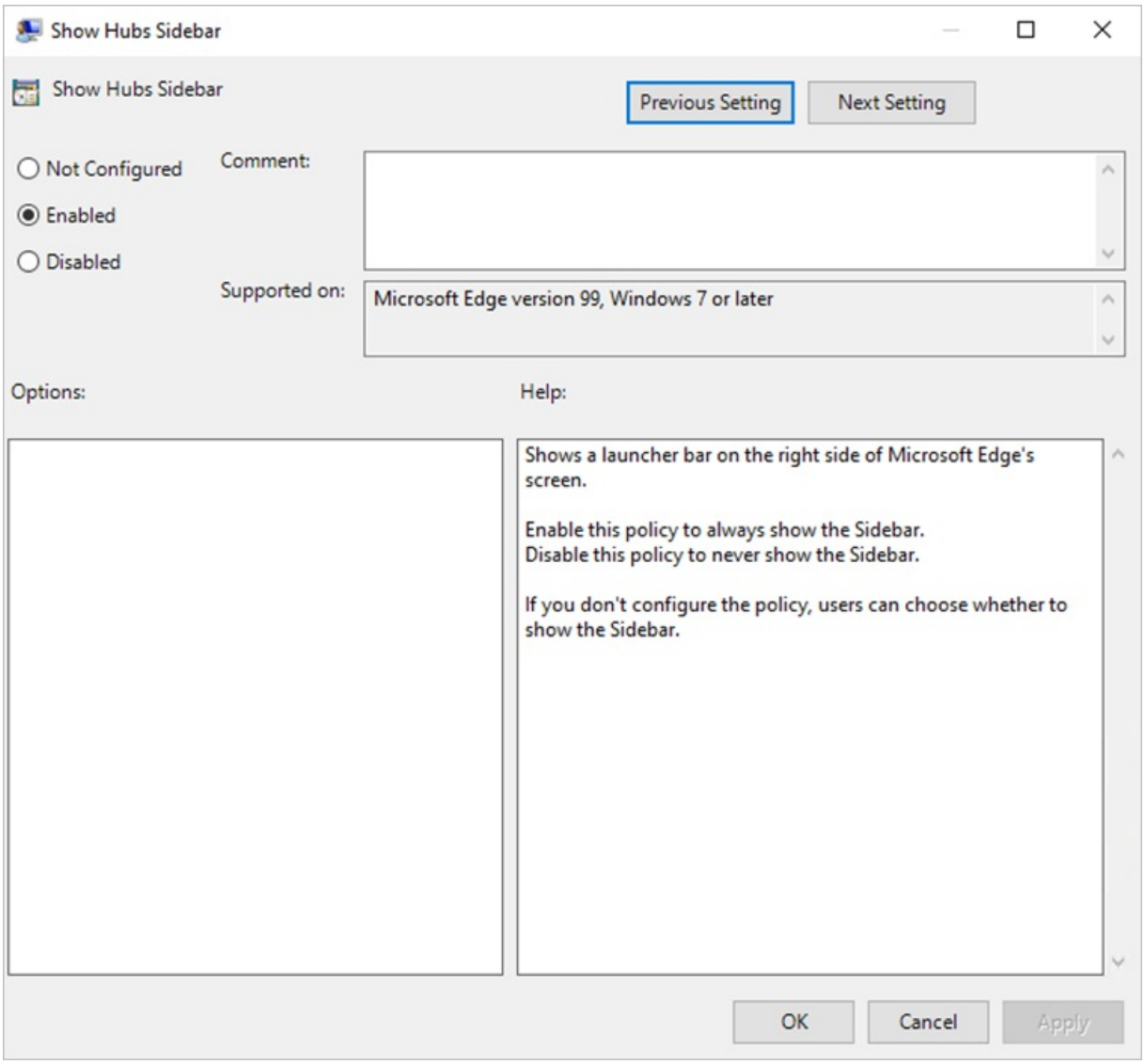
POLICY NAME	CAPTION
HubsSidebarEnabled	Show Hubs Sidebar
ExtensionInstallBlockList	Control which extensions cannot be installed
ExtensionInstallForceList	Control which extensions are installed silently

> **NOTE**
> The reuse of Extensions-specific policies for managing the sidebar is intentional and intended to promote flexibility. Navigate to *edge://sidebar-internals* in your browser to find the extension IDs associated with individual sidebar apps.

Allow or block the sidebar in group policy

You can use HubsSidebarEnabled policy to control whether the sidebar is allowed or blocked in your organization. Blocking the sidebar will automatically block all sidebar apps from being enabled.

1. Open the group policy editor and go to **Administrative Templates** > **Microsoft Edge** and then select **Show Hubs Sidebar**.
2. To block the sidebar and all sidebar apps, select **Disabled**.
3. To allow the sidebar, select **Enabled**.



Block specific sidebar apps

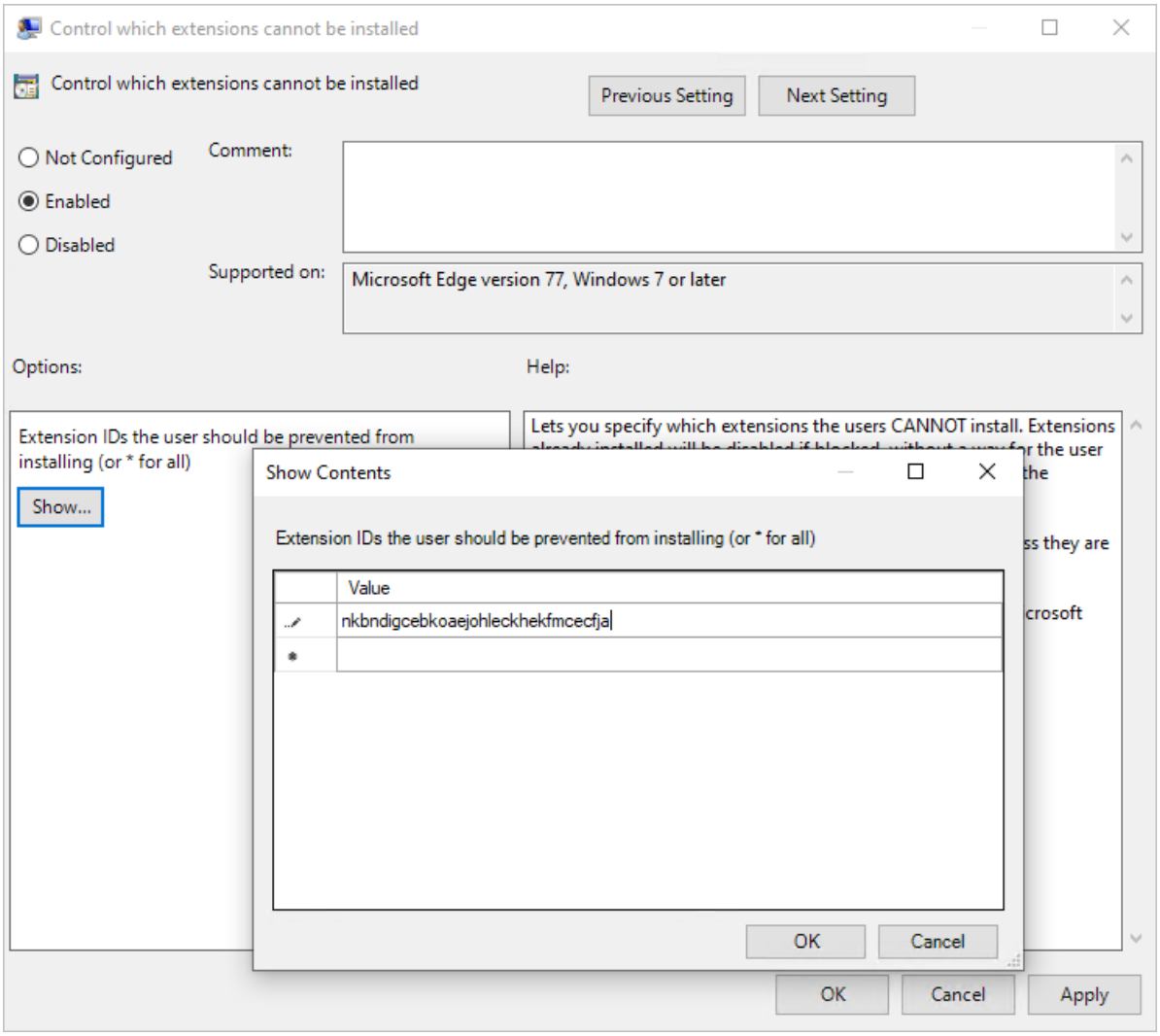
You can use the ExtensionInstallBlockList policy to control which sidebar apps are blocked.

> **NOTE**
> During the rollout of Microsoft Edge 107, the following sidebar app experiences are turned on by default for Enterprise customers: Search, Discover, Office.com, and Outlook.
> Admins can use the following guidance to reconfigure the sidebar as desired for their organization.

Use the following steps as a guide to block a sidebar app.

1. Open the group policy management editor and go to **Administrative Templates** > **Microsoft Edge** > **Extensions** and then select **Control which extensions cannot be installed**.
2. Select **Enabled**.
3. Click **Show**.
4. Enter the extension ID of the sidebar app that you want to block.
   - You can find Extension IDs for sidebar apps by going *edge://sidebar-internals*.
   - The Sidebar Internals JSON file includes a manifest for all sidebar apps, including an `extension_id` parameter for each app. You can use these values to configure the policy.
   - When adding multiple ID's use a separate row for each ID.
5. To block all sidebar apps, refer to Allow or block the sidebar in group policy. Disabling the

HubsSidebarEnabled policy will block all sidebar apps by default.



Force enable specific sidebar apps

Use the ExtensionInstallForceList policy to enable specific sidebar apps that can't be disabled by users in your organization. Use the following steps as a guide to force enable a sidebar app.

1. In the Group Policy Editor, go to **Administrative Templates** > **Microsoft Edge** > **Extensions** and then select **Control which extensions are installed silently**.
2. Select **Enabled**.
3. Click **Show**.
4. Enter the extension ID(s) for the sidebar apps you want to force enable.

The sidebar app will be enabled silently without needing any user interaction. The user won't be able to remove this app from the sidebar. This setting will overwrite any blocklist policy that's enabled.

See also

- Microsoft Edge Enterprise landing page

Use group policies to manage Microsoft Edge extensions

11/1/2022 • 6 minutes to read • Edit Online

This article describes the options and steps for managing extensions by using group policies. These options assume that you already have Microsoft Edge managed for your users. If you have not already set up Microsoft Edge to be managed for your users please follow the below link to do so now.

- Manage Microsoft Edge extensions in the enterprise

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

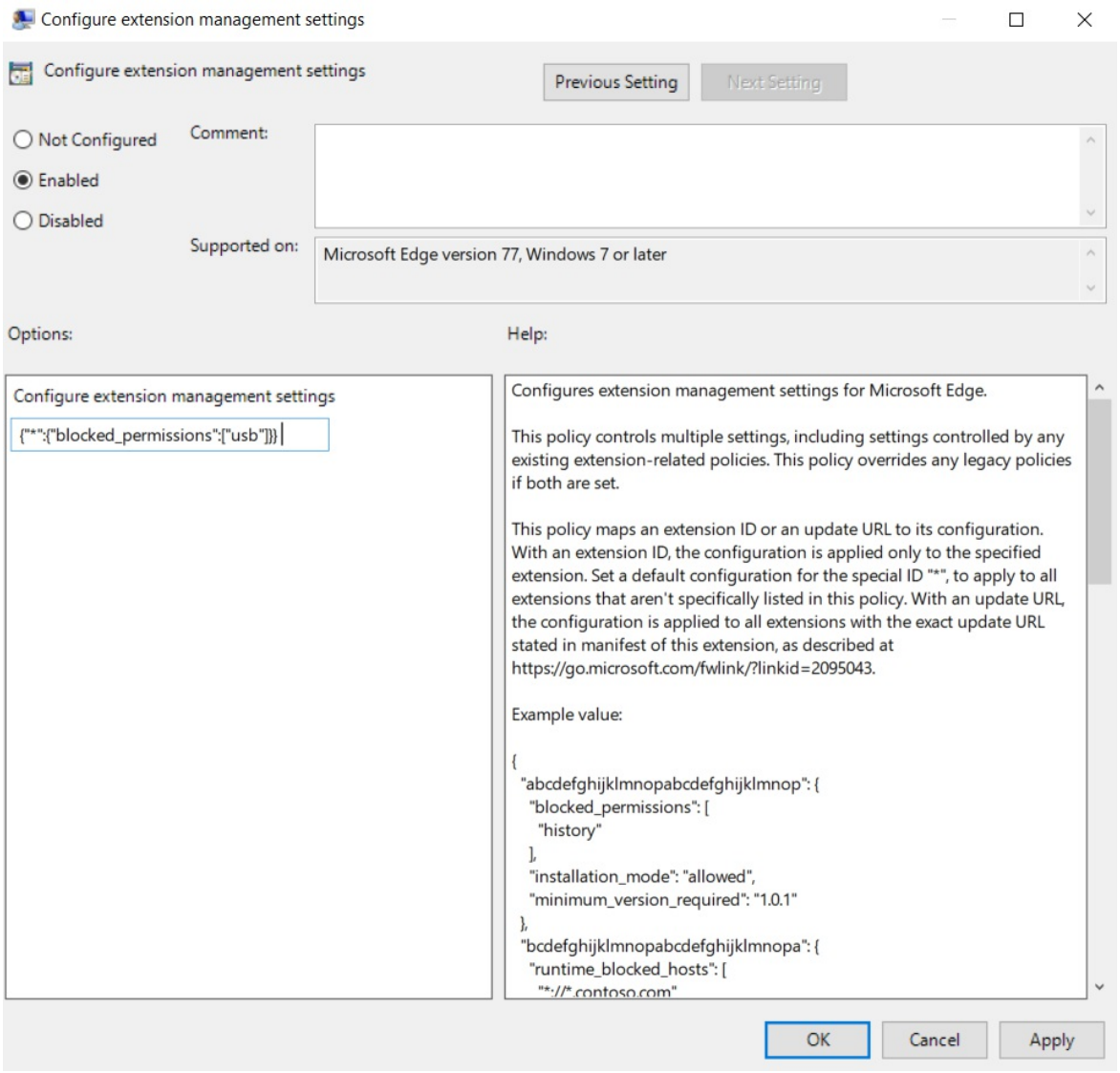
Block extensions based on their permissions

You can control what extensions your users can install based on permissions using the ExtensionSettings policy. If an installed extension needs a permission that's blocked, it just won't run. The extension isn't removed, just disabled.

> **NOTE**
> The blocked permissions setting can only be set within the extension settings policy.

Use the following steps as a guide for blocking an extension.

1. Open the group policy management editor and go to **Administrative Templates > Microsoft Edge > Extensions** and then select **Configure extension management settings**.
2. Enable the policy, then enter the permissions that you want allowed or blocked, by using a JSON string that gets compressed. The next screenshot shows how to block an extension that uses the permission "usb".


Configure extension management settings
Configure extension management settings
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
Microsoft Edge version 77, Windows 7 or later
Options:
Help:
Configure extension management settings
{"*":{"blocked_permissions":["usb"]}}
Configures extension management settings for Microsoft Edge.
This policy controls multiple settings, including settings controlled by any existing extension-related policies. This policy overrides any legacy policies if both are set.
This policy maps an extension ID or an update URL to its configuration. With an extension ID, the configuration is applied only to the specified extension. Set a default configuration for the special ID "*", to apply to all extensions that aren't specifically listed in this policy. With an update URL, the configuration is applied to all extensions with the exact update URL stated in manifest of this extension, as described at https://go.microsoft.com/fwlink/?linkid=2095043.
Example value:
{
"abcdefghijklmnopabcdefghijklmnop": {
"blocked_permissions": [
"history"
],
"installation_mode": "allowed",
"minimum_version_required": "1.0.1"
},
"bcdefghijklmnopabcdefghijklmnopa": {
"runtime_blocked_hosts": [
OK
Cancel
Apply

The following example shows the JSON to block any extension that needs the use of permission "usb" and its compressed string.

JSON example

```
{
     "*": {
          "blocked_permissions": ["usb"]
     }
}
```

```
{"*":{"blocked_permissions":["usb"]}}
```

> **NOTE**
> To block all extensions that use the permission, use an asterisk for the extension ID, as shown in the previous example. If you specify one extension ID, the policy will only apply to that extension. You can block more than one, but they need to be separate entries.

Prevent extensions from altering web pages

This setting prevents extensions from reading and changing data from sensitive websites and domains. Blocking unwanted actions is done by blocking actions such as script injection into your websites, reading the cookies, or

making web-request modifications. This setting doesn't prevent your users from installing or removing extensions, it only prevents extensions from altering the specified websites.

> **NOTE**
> The Runtime allowed/blocked hosts setting can only be set within the extension settings policy.

You can configure the following settings in the ExtensionSettings policy to prevent (or allow) alterations of websites or domains:

- **Runtime_blocked_hosts**. This setting blocks extensions from making changes or reading data from the websites you specify.
- **Runtime_allowed_hosts**. This setting allows extensions to make changes or read data from the websites you specify. The following format is used for specifying your site(s) in the JSON string in the policy:

  ```
  [http|https|ftp|*]://[subdomain|*].[hostname|*].[eTLD|*] [http|https|ftp|*],
  ```

  > **NOTE**
  > `[hostname|*], and [eTLD|*]` sections are required, but `[subdomain|*]` section is optional.

The following table shows examples of valid host patterns and matching patterns.

VALID HOST PATTERNS	MATCHES	DOESN'T MATCH
`*://*.example.*`	`http://example.com` `https://test.example.co.uk`	`https://example.microsoft.com` `http://example.microsoft.co.uk`
`http://example.*`	`http://example.com` `http://example.ly`	`https://example.com` `http://test.example.com`
`http://example.com`	`http://example.com`	`https://example.com` `http://test.example.co.uk`
`*://*`	All URLs	

Use the following steps as a guide to block or allow extensions to access a website or domain.

1. Open the group policy management editor and go to **Administrative Templates > Microsoft Edge > Extensions**, and then select **Configure extension management settings**.
2. Enable the policy, then enter the permissions that you want allowed or blocked, compressing the permissions to a single JSON string.

The following examples show how to block extensions on a hostname and how to block extensions on the same domain.

JSON example to block hostname

This example shows the JSON and compressed JSON string to block any extension from accessing the `www.microsoft.com` hostname.

```
{
    "*":{
            "runtime_blocked_hosts":["www.microsoft.com"]
    }
}
```

```
{"*":{"runtime_blocked_hosts":["www.microsoft.com"]}}
```

> **NOTE**
> To block all extensions from accessing a webpage, use an asterisk for the extension ID, as shown in the previous example. If you specify one extension ID instead of an asterisk, the policy will only apply to that extension. You can block more than one extension, but they need to be separate entries.

JSON example to block extensions on same domain

This example shows the JSON and compressed JSON string to block specific extensions from running on the same domain, "importantwebsite".

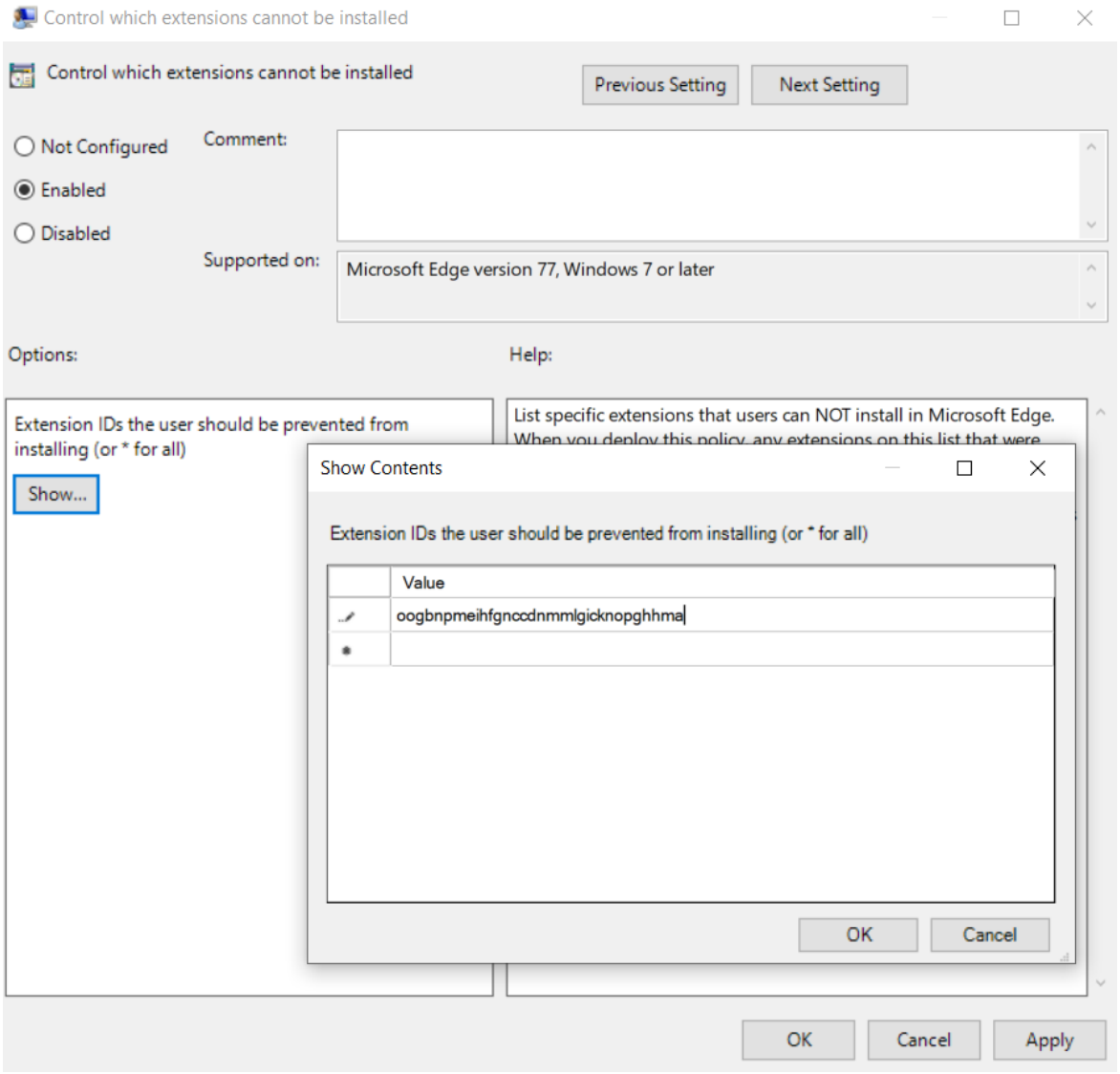
```
{
    "aapbdbdomjkkjkaonfhkkikfgjllcleb": {
        "runtime_blocked_hosts": ["*://*.importantwebsite"]
    },
    "bfbmjmiodbnnpllbbbfblcplfjjepjdn": {
        "runtime_blocked_hosts": ["*://*.importantwebsite"]
    }
}
```

```
{"aapbdbdomjkkjkaonfhkkikfgjllcleb": {"runtime_blocked_hosts":
["*://,*.importantwebsite"]},"bfbmjmiodbnnpllbbbfblcplfjjepjdn": {"runtime_blocked_hosts":
["*://*.importantwebsite"]}}
```

Allow or block extensions in group policy

You can use the ExtensionInstallBlocklist and ExtensionInstallAllowlist policies to control which extensions are blocked or allowed. Use the following steps as a guide to allow all extensions except those you want to block.

1. Open the group policy management editor and go to **Administrative Templates > Microsoft Edge > Extensions** > and then select **Control which extensions cannot be installed**.
2. Select **Enabled**.
3. Click **Show**.
4. Enter the app ID of the extensions that you want to block. When adding multiple app ID's use a separate row for each ID.
5. To block all extensions, type * into the policy to prevent any extensions from being installed. You can use this in conjunction with the "Allow specific extensions to be installed" policy to only allow certain extensions to be installed. The next screenshot shows an extension that will be blocked based on the app ID that's provided.



TIP

If you can't find the app ID of an extension, look at the extension in the Microsoft Edge Add-ons website. Find the specific extension and you will see the app ID at the end of the URL in the omnibox.

NOTE

You can add an extension to the blocklist that's already installed on a user's computer. This will disable the extension and prevent the user from re-enabling it. It won't be uninstalled, just disabled.

Force-install an extension

Use the ExtensionInstallForcelist policy to control which extensions are blocked or allowed. Use the following steps as a guide to force-install an extension.

1. In the Group Policy Editor, go to **Administrative Templates> Microsoft Edge > Extensions >** and then select **Control which extensions are installed silently**.
2. Select **Enabled**.
3. Click **Show**.
4. Enter the app ID or IDs of the extension or extensions you want to force-install.

The extension will be installed silently with no need for user interaction. The user also won't be able to uninstall

or disable the extension. This setting will overwrite over any blocklist policy that's enabled.

> **NOTE**
> For extensions hosted in the Chrome web store use a string such as: `pckdojakecnhhplcgfflhndiffaohfah;https://clients2.google.com/service/update2/crx`. For self-hosted extensions use the pattern extension_id;update_url where update_url points to the location of the update manifest XML file. For example, `mfjlfjaknfckffgjgmdfeheeealceoak;https://file_location.azurewebsites.net/picture_of_the_day.xml`.

Block extensions from a specific store or update URL

To block extensions from a particular store or URL, you only need to block the *update_url* for that store using the ExtensionSettings policy.

Use the following steps as a guide to block extensions from an particular store or URL.

1. Open the group policy management editor and go to **Administrative Templates > Microsoft Edge > Extensions >** and then select **Configure extension management settings**.
2. Enable the policy, then enter the permissions that you want allowed or blocked, compressing it to a single JSON string.

The next example shows the JSON and compressed JSON string to block from the Chrome Web Store using its update URL (`https://clients2.google.com/service/update2/crx`).

JSON example for blocking on update URL

```
{
"update_url:https://clients2.google.com/service/update2/crx":{
                                                              " installation_mode":"blocked"
                                                              }
}
```

```
{"update_url:https://clients2.google.com/service/update2/crx":{"installation_mode":"blocked"}}
```

> **NOTE**
> You can still use **ExtensionInstallForceList** and **ExtensionInstallAllowList** to allow/force install specific extensions even if the store is blocked using the JSON in the previous example.

See also

- Manage Microsoft Edge extensions in the enterprise
- Create a web store to host Microsoft Edge extensions
- Reference guide for the ExtensionSettings policy
- FAQ for Microsoft Edge Extensions
- Microsoft Edge Enterprise landing page

Self-host Microsoft Edge extensions

11/1/2022 • 4 minutes to read • Edit Online

This article provides basic guidance for packaging an extension to host on your own webstore. It also includes instructions on how to deploy extensions to devices and users in your organization.

Prerequisites

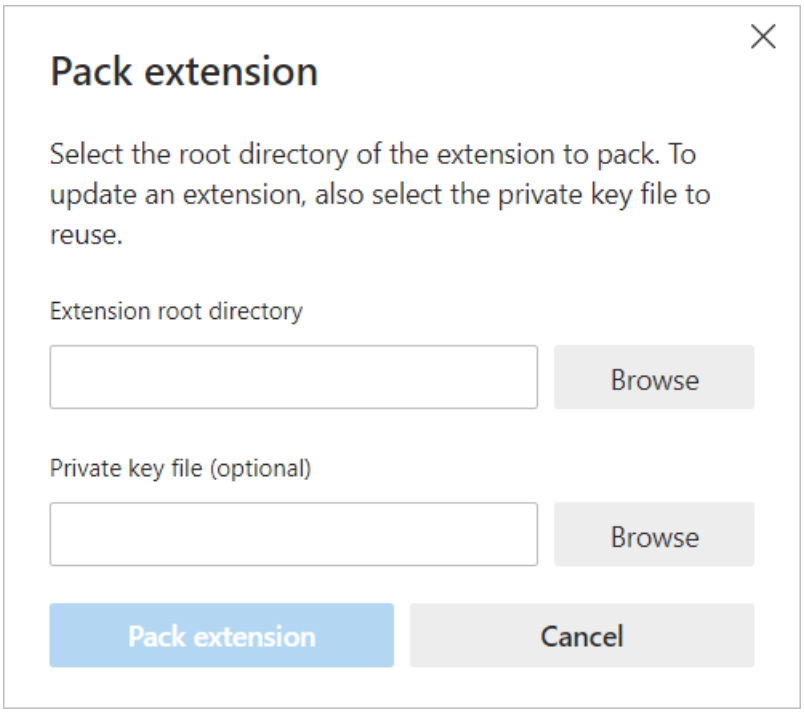
To self-host your own extensions, you will need to provide your own web hosting services for the extensions and their manifest files.

The following steps assume that you've already created your extension, have some experience with XML files, have a working knowledge of configuring group policy, and know how to use the Windows registry.

Publish an extension

Before you publish an extension it needs to be packed into a CRX (Chrome extension) file. Use the following steps as a guide to packing an extension as a CRX file.

1. In the Microsoft Edge address bar, go to *edge://extensions* and turn on **Developer mode** if it's not already enabled.
2. Under **Installed extensions**, click **Pack Extension** to create the CRX file.
3. Use the **Pack extension** dialog to find the directory that has the source for the extension. Select the directory and then click **Pack extension**. This will create your CRX file, along with a PEM file. Save the PEM file because it's needed for making version updates to the extension. The next screenshot shows the **Pack extension** dialog for locating the root directory of the extension.

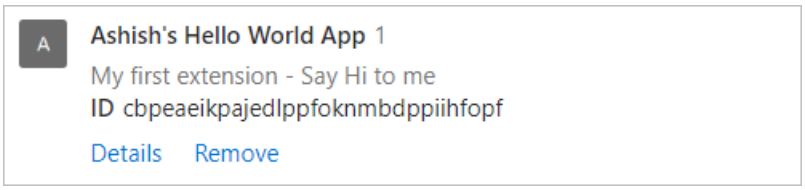

Pack extension
Select the root directory of the extension to pack. To update an extension, also select the private key file to reuse.
Extension root directory
Browse
Private key file (optional)
Browse
Pack extension
Cancel

IMPORTANT

Store the PEM file in a safe location because it's the key for the extension and it's needed for future updates.

4. Drag the CRX file into your extensions window and make sure that it loads.

5. Test the extension and take note of the ID field (this is the CRX ID) and version number. You'll need this information later. The next screenshot shows a test extension with its CRX ID.



6. Upload the the CRX file to the host and note the URL of the location it will be downloaded from. This information is needed for the XML manifest file.

7. To create a manifest XML file with the app/extension ID, download URL, and version, define the following fields:

   - **appid** - The extension ID from step 5
   - **codebase** - The download location for the CRX file from step 6
   - **version** - The version of the app/extension, which should match the version specified in the manifest of the extension.

   The next code snippet shows an example of an XML manifest file.

```
<?xml version='1.0' encoding='UTF-8'?>
<gupdate xmlns='http://www.google.com/update2/response' protocol='2.0'>
  <app appid='ekilpdeokbpjmminmhfcgkncmmohmfeb'>
  <updatecheck codebase='https://app.somecompany.com/extensionfolder/helloworld.crx' version='1.0' />
  </app>
</gupdate>
```

   For more information, see Auto-update extensions in Microsoft Edge - Microsoft Edge Development.

8. Upload the completed XML file to a location where it can be downloaded from, noting the URL. This URL will be needed when you install the extension using a group policy. See Distribute a privately hosted extension.

> **IMPORTANT**
> The hosting location for the extension doesn't need authentication. It needs to be accessible by user devices wherever they might be used.

Publish updates to an extension

After you change and test the updated extension you can publish it. Use the following steps as a guide for publishing an update.

1. Change the version number in your extension's manifest.JSON file to a higher number using the following syntax: `"version":"versionString"`. If the "version":"1.0", then you can update to "version":"1.1" or any number higher than "1.0".

2. Update the "version" of `<updatecheck>` in the XML file to match the number that you put in the manifest file in the previous step. For example:
   `<updatecheck codebase='https://app.somecompany.com/extensionfolder/helloworld.crx' version='1.1' />`

3. Create a CRX file that includes the new changes. Go to *edge://extensions* and enable **Developer mode**.

4. Click **Pack extension** and go to the directory for the extension source.

   > **IMPORTANT**
   > Use the same PEM file that was generated and saved the first time the CRX file was created. If you don't use the same PEM file the app ID of the extension will change and the update will be treated as a new extension.

5. Drag and drop the CRX file into the extensions window and verify that it loads. The extension will be disabled after this operation. To enable it add the CRX ID of the extension to the ExtensionInstallAllowList policy.

6. Test the updated extension.

7. Replace the old CRX file and XML file with the new files for the updated extension.

The extension's changes will be picked up during the next policy sync cycle. For more information about updating extensions, see: Update URL and Update manifest.

Distribute a privately hosted extension

You can share the link of the location where the CRX file is hosted, and as soon as users enter the URL in their browser the extension will be downloaded and installed. Users can enable the extension from the edge://extensions page. To allow users to install self-hosted extensions, you need to add the extension CRX IDs to the ExtensionInstallAllowList policy and add the URL of the location where the CRX file is hosted to the ExtensionInstallSources policy.

Alternatively, you can use group policy ExtensionInstallForceList to Force-install an extension on your users' devices.

You can apply these policies to your selected users, devices, or both. Remember though that policy updates are not instantaneous, and it will take time for the policy settings to take effect.

See also

- Manage Microsoft Edge extensions in the enterprise
- Use group policies to manage Microsoft Edge extensions
- Detailed guide to the ExtensionSettings policy
- FAQ for Microsoft Edge Extensions
- Microsoft Edge Enterprise landing page

A detailed guide to configuring extensions using the ExtensionSettings policy

11/1/2022 • 8 minutes to read • Edit Online

Microsoft Edge offers multiple ways to manage extensions. A common way is to set multiple policies in one place with a JSON string in the Windows Group Policy Editor or in the Windows Registry using the ExtensionSettings policy.

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

Before you begin

Decide if you want to set all extension management settings in the ExtensionSettings policy or set these controls through other policies.

The ExtensionSettings policy can overwrite other policies that you've set elsewhere in group policy, including the following policies:

- ExtensionAllowedTypes
- ExtensionInstallBlocklist
- ExtensionInstallForcelist
- ExtensionInstallSources
- ExtensionInstallAllowlist

ExtensionSettings policy fields

This policy can control settings such as Update URL, where the extension will be downloaded from for initial install, and Blocked permissions. You can also use this policy to identify which permissions aren't allowed to run. The available policy fields are described in the following table.

POLICY FIELD	DESCRIPTION
allowed_types	Can only be used to configure the default configuration,*. Specifies what types of app or extension users are allowed to install on Microsoft Edge. The value is a list of strings, each of which should be one of the following types: "extension", "theme", "user_script", and "hosted_app".
blocked_install_message	If you block users from installing certain extensions, you can specify a custom message to display in the browser if users try to install them. Append text to the generic error message that is displayed on the Microsoft Edge Add-ons website. For example, you can tell users how to contact their IT department or why a particular extension is unavailable. The message can be up to 1,000 characters long.

POLICY FIELD	DESCRIPTION
blocked_permissions	Prevents users from installing and running extensions that request certain API permissions that your organization doesn't allow. For example, you can block extensions that access cookies. If an extension requires a permission that you blocked, the users can't install it. If users previously installed the extension, it will no longer load. If an extension contains a blocked permission as an optional requirement, it installs as usual. Then, while the extension is running, blocked permissions are automatically declined. For a list of available permissions, see declare permissions.
installation_mode	Controls if and how extensions that you specify are added to Microsoft Edge. You can set the installation mode to one of the following options: - `allowed`: Users can install the extension. If no installation mode is defined, this setting is the default. - `blocked`: Users can't install the extension. - `force_installed`: Automatically install the extension without user interaction. Users can't remove it. You also need to define the extension download location using "update_url". **Note**: You can't usethis setting with *because Microsoft Edge wouldn't know which extension to automatically install. - `normal_installed`: Automatically install the extension without user interaction. Users can disable it. You also need to define the extension download location using "update_url". **Note**: You can't usethis setting with *because Microsoft Edge wouldn't know which extension to automatically install. - `removed`: Users can't install the extension. If users previously installed the extension, Microsoft Edge removes it.
install_sources	Can be used only to configure the default configuration,*. Specifies which URLs are allowed to install extensions. Both the location of the *.crx file and the page where the download is started from (the referrer) must be allowed by these patterns. For URL pattern examples, see the match patterns.
minimum_version_required	Microsoft Edge disables extensions, including force-installed extensions, with a version older than the specified minimum version. The format of the version string is the same as the one used in the extension manifest.
update_url	Only applies to `force_installed` and `normal_installed`. Specifies where Microsoft Edge should download an extension from. If the extension is hosted in the Microsoft Edge Add-ons website, use this location: `https://edge.microsoft.com/extensionwebstorebase/v1/crx`. Microsoft Edge uses the URL that you specify for the initial extension installation. For subsequent extension updates, Microsoft Edge uses the URL in the extension's manifest.

POLICY FIELD	DESCRIPTION
runtime_allowed_hosts	Allows extensions to interact with specified websites, even if they're also defined in runtime_blocked_hosts. You can specify up to 100 entries. Extra entries are discarded. The host pattern format is similar tomatch patternsexcept you can't define the path. For example: - *://*example.com - *://example.*—eTLD wildcards are supported
runtime_blocked_hosts	Prevent extensions from interacting with or modifying websites that you specify. Modifications include blocking JavaScript injection, cookie access, and web-request modifications. You can specify up to 100 entries. Extra entries are discarded. The host pattern format is similar to match patterns ex'cept you can't define the path. For example: - *://*example.com - *://example.*—eTLD wildcards are supported
override_update_url	Available from Microsoft Edge 93 If this field is set to `true`, Microsoft Edge uses the update URL specified in the ExtensionSettings policy or in the ExtensionInstallForcelist policy, for subsequent extension updates. If this field isn't set or is set to `false`, Microsoft Edge uses the URL specified in the extension's manifest for updates.
toolbar_state	Available from Microsoft Edge 103 This policy setting lets you force show an installed extension to the toolbar. The default state is `default_hidden` for all extensions. The following values are possible for this setting: - `force_shown`: You can choose to force show an installed extension on the toolbar. Users won't be able to hide the specified extension icon from the toolbar. - `default_hidden`: This is the default setting for all the installed extensions on the browser. - `default_shown`: In this state, extensions are shown on the toolbar on installation. Users can hide them from the toolbar, if needed.

The following keys are allowed at the global scope (*):

- blocked_permissions
- installation_mode - only `"blocked"`, `"allowed"`, or `"removed"` are the valid values in this scope.
- runtime_blocked_hosts
- blocked_install_message
- allowed_types
- runtime_allowed_hosts
- install_sources

The following keys are allowed at an individual extension scope:

- blocked_permissions
- minimum_version_required
- blocked_install_message
- installation_mode - `"blocked"`, `"allowed"`, `"removed"`, `"force_installed"`, and `"normal_installed"` are the possible values.

- runtime_allowed_hosts
- update_url
- override_update_url
- runtime_blocked_hosts
- toolbar_state

The following keys are allowed at an update URL scope:

- blocked_permissions
- installation_mode - only `"blocked"`, `"allowed"`, or `"removed"` are the valid values in this scope.

Configure using a JSON string in Windows Group Policy Editor

The steps to use the extension settings policy using GPO assume that you've already imported the ADM/ADMX for Microsoft Edge Policies.

1. Open the group policy editor and go to **Microsoft Edge > Extensions > Configure extension management setting policy**.
2. Enable the policy and enter its compact JavaScript Object Notation (JSON) data in the text box as a single line without line breaks.
3. To validate the policy and compact it into a single line, use a JSON compression tool.

Properly format JSON for the extension settings policy

You need to understand the two parts to this policy—the default scope and the individual scope. The default scope is a catch-all for extensions without their own scope. The individual scope is applied to that extension only.

The default scope is identified by the asterisk (*). The next example defines a default scope and an individual extension scope.

```
{
   "*": {},
   "nckgahadagoaajjgafhacjanaoiihapd": {}
}
```

An extension will only get its settings from one scope. If there's an individual extension scope for that extension, those will be the settings that apply to that extension. If no individual extension scope exists, then the extension will use the default scope.

The next JSON example blocks any extension from running on `.example.com` and blocks any extension that requires the permission "USB".

```
{
  "*": {
    "runtime_blocked_hosts": ["*://*.example.com"],
    "blocked_permissions": ["usb"]
  }
}
```

Compact JSON

```
{"*":{"runtime_blocked_hosts":["*://*.example.com"],"blocked_permissions":["usb"]}}
```

A few more JSON examples for extension settings

Using installation_mode property to allow and block extensions

- User can install all extensions - the default setting

```
{ "*": {"installation_mode": "allowed" }}
```

- User can't install any extensions.

```
{ "*": {"installation_mode": "blocked" }}
```

- Specify a custom message to display when installation is blocked.

```
{"*": {"blocked_install_message": ["Call IT(408 - 555 - 1234) for an exception"]}}
```

Using installation_mode property to force install extensions

When using installation_mode as "force_installed", the extension is automatically installed without user interaction. A user can't disable or remove the extension. If an extension is "normal" or "force" installed, the **update_url** field must also be defined. This field points to the location where the extension can be installed from. Use the following locations for the **update_url** field:

- If the extension you're downloading is hosted on the Microsoft Edge Add-ons store, use the location in the following JSON example:

```
{"nckgahadaanghapdoaajjgafhacjaoii": {"installation_mode": "force_installed","update_url":
"https://edge.microsoft.com/extensionwebstorebase/v1/crx"}}
```

- If the extension you're downloading is hosted on the Chrome Web Store, use the location in the following JSON example:

```
{"nckgiihapdoaajjgafhacjgahadaanao": {"installation_mode": "force_installed","update_url":
"https://clients2.google.com/service/update2/crx"}}
```

- If you're hosting the extension on your own server, use the URL where Microsoft Edge can download the packed extension (.crx file). JSON example:

```
{"nckgahadagoaajjgafhacjanaoiihapd": {"installation_mode": "force_installed","update_url":
"https://edge.microsoft.com/extensionwebstorebase/v1/crx"}}
```

In the previous example, if you use "normal_installed" instead of "force_installed", then the extension is automatically installed without user interaction, but they can disable the extension.

> **TIP**
> Formatting a JSON string correctly can be tricky. Use a JSON checker before implementing the policy. Or try the early version of Extension Settings Generator Tool

Configure using the Windows Registry

The ExtensionSettings policy should be written to the registry under this key:

```
HKLM\Software\Policies\Microsoft\Edge\
```

> **NOTE**
> It's possible to use HKCU instead of HKLM. The equivalent path can be configured with Group Policy Object (GPO).

For Microsoft Edge, all settings will start under this key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\
```

The next key that you'll create is either the Extension ID for individual scope or an asterisk (*) for the Default Scope. For example, you'd use the following location in the registry for settings that apply to Google Hangouts:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\ExtensionSettings\nckgahadagoaajjgafhacjanaoiihapd
```

For settings that apply to the Default Scope (asterisk), use the following location in the registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\ExtensionSettings\*
```

Different settings will require different formats, depending on whether they're a string or an array of strings. Array values require [" value "]. String values can be entered as is. The following list shows which settings are arrays or strings:

- Installation_mode = String
- update_url = String
- blocked_permissions = Array of strings
- allowed_permissions = Array of Strings
- minimum_version_required = String
- runtime_blocked_hosts = Array of strings
- runtime_allowed_hosts = Array of Strings
- blocked_install_message = String

See also

- Manage Microsoft Edge extensions in the enterprise
- Use group policies to manage Microsoft Edge extensions
- FAQ for Microsoft Edge Extensions
- Microsoft Edge Enterprise landing page

FAQ for Microsoft Edge extensions

11/1/2022 • 2 minutes to read • Edit Online

This article provides an FAQ for Microsoft Edge extensions.

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

What is the update URL for the Microsoft Edge Add-ons store?

The update URL for extensions hosted on Microsoft Edge Add-ons is: https://edge.microsoft.com/extensionwebstorebase/v1/crx.

What is the update URL for Chrome Web Store extensions?

The update URL for extensions hosted on Chrome Webstore is: https://clients2.google.com/service/update2/crx

See also

- Manage Microsoft Edge extensions in the enterprise
- Use group policies to manage Microsoft Edge extensions
- Create a web store to host Microsoft Edge extensions
- Reference guide for the ExtensionSettings policy
- Microsoft Edge Enterprise landing page

Configure Microsoft Edge enterprise sync

11/1/2022 • 4 minutes to read • Edit Online

This article explains how admins can configure Microsoft Edge to sync user favorites, passwords, and other browser data across all signed-in devices.

> **NOTE**
> Applies to Microsoft Edge on Chromium, version 77 or later unless otherwise noted.

Introduction

Microsoft Edge sync enables users to access their browsing data across all their signed-in devices. Users can sync the following data:

- Favorites
- Passwords
- Addresses and more (form-fill)
- Collections
- Settings
- Extensions
- Open tabs (available in Microsoft Edge version 88 or later)
- History (available in Microsoft Edge version 88 or later)

> **NOTE**
> Additional device connectivity and configuration data (such as device name, device make, and device model) is uploaded to support sync functionality.

Sync functionality and user sync configuration

After sync is configured, sync functionality is enabled via user consent. Users can turn sync on or off for each of the supported data types. For more information, see Sign in to sync Microsoft Edge across devices.

> **NOTE**
> If a user is experiencing a sync issue, they might need to reset sync in **Settings** > **Profiles** > **Sync** > **Reset sync**.

Prerequisites

The following prerequisites apply to Microsoft Edge enterprise sync:

- Microsoft Edge version that supports the desired sync functions
- Subscription to a cloud service in a supported environment
- Azure Information Protection (AIP) (P1 or P2)

Supported environments

Microsoft Edge sync for Azure Active Directory (Azure AD) accounts is available for any of the following

subscriptions:

- Azure AD Premium (P1 or P2)

  > **NOTE**
  > Customers that only have Azure AD P1 or P2 must enable Azure AD Enterprise State Roaming (ESR). Microsoft Edge sync isn't part of ESR, but ESR is required to provide the AIP functionality that's needed for the P1 and P2 configurations. To learn more, see the Enable Enterprise State Roaming in Azure Active Directory article.

- Microsoft 365 Business Premium, Business Standard, or Business Basic

  > **NOTE**
  > Business Basic is supported, but some existing tenants need to be backfilled with the RMS_S_BASIC service plan needed by AIP. Customers can file a support request if they need to backfill a tenant.

- Office 365 E1 and above
- All EDU subscriptions, including:
  - Microsoft Apps for Students or Faculty
  - Exchange Online for Students or Faculty
  - O365 A1 or above
  - Microsoft 365 A1 or above
  - Azure Information Protection P1 or P2 for Students or Faculty

Sync group policies

Admins can use the following group policies to configure and manage Microsoft Edge sync:

- SyncDisabled: Disables data synchronization. This policy disables cloud synchronization only and has no effect on the RoamingProfileSupportEnabled policy.
- SavingBrowserHistoryDisabled: Disables saving browsing history and sync and open tabs sync.
- AllowDeletingBrowserHistory: When this policy is set to disabled, history sync will also be disabled.
- SyncTypesListDisabled: Configure the list of data types that are excluded from synchronization. Use this policy to limit the type of data uploaded to the Microsoft Edge synchronization service.
- RoamingProfileSupportEnabled: Allow Active Directory (AD) profiles to use on-premises storage. The settings stored in Microsoft Edge profiles (favorites and preferences) are also saved to a file stored in the Roaming user profile folder (or the location specified by the administrator.) For more information, see On-premises sync for Active Directory (AD) users.
- ForceSync: Force synchronization of browser data and don't show the sync consent prompt. Users can't disable this policy.

Use Azure Information Protection to configure Microsoft Edge sync

Configuration options for Microsoft Edge sync are available through the Azure Information Protection (AIP) service. When AIP is enabled for a tenant, all users can sync Microsoft Edge data, regardless of licensing. The protection service might be activated automatically, by using PowerShell, or by using the Azure portal. For more information and instructions on how to enable AIP, see Activating the protection service from Azure Information Protection (AIP).

Caution

Activating Azure Information Protection will also allow other applications, such as Microsoft Word or Microsoft

Outlook, to protect content with AIP. Any onboarding control policy that's used to restrict Microsoft Edge sync will also restrict other applications from protecting content using AIP.

Control user onboarding for a phased deployment

You can use the Set-AipServiceOnboardingControlPolicycmdlet to set the policy that controls user on-boarding for Azure Information Protection. If sync still isn't available after all the specified users are onboarded, ensure that the IPCv3Service is enabled using the Get-AIPServiceIPCv3 PowerShell cmdlet. For more information, see Configuring onboarding controls for a phased deployment.

Microsoft Edge and Enterprise State Roaming (ESR)

Microsoft Edge is a cross-platform application with an expanded scope for syncing user data across all their devices and is no longer a part of Azure AD Enterprise State Roaming. However, Microsoft Edge will fulfill the data protection promises of ESR, such as the ability to bring your own key. For more information, see Microsoft Edge and Enterprise State Roaming.

See also

- Diagnose and fix Microsoft Edge sync issues
- Microsoft Edge enterprise sync FAQ
- Microsoft Edge and Enterprise State Roaming
- What is Azure Information Protection?
- Microsoft Edge Enterprise landing page

Diagnose and fix Microsoft Edge sync issues

11/1/2022 • 6 minutes to read • Edit Online

This article provides troubleshooting guidance for the most common sync issues in an Azure Active Directory (Azure AD) environment. It also includes troubleshooting steps and the recommended tools for gathering the logs needed for troubleshooting a sync issue.

If a user is experiencing an issue syncing browser data across their devices, they can reset sync in **Settings** > **Profiles** > **Sync** > **Reset sync**. If the sync reset doesn't work, an admin or support staff member can use the guidance in this article to fix a sync issue.

> **NOTE**
> Applies to Microsoft Edge on Chromium, version 77 or later unless otherwise noted.

Before you begin: identity issues versus sync issues

It's important to understand the difference between identity issues and sync issues. A popular use case for maintaining user identity in the browser is to support sync. For this reason, identity issues are frequently confused with sync issues. Understand the difference between identity and sync issue before you start troubleshooting sync.

Before you treat an issue as a sync issue, check to see if the user is signed into the browser with a valid account.

The next screenshot shows an example of an identity error. The error is **Last Token Error, EDGE_AUTH_ERROR: 3, 54, 3ea**, which is found in *edge://sync-internals* under **Credentials**.

Credentials

Requested Token	2020-12-29 10:10:03 -06
Received Token Response	2020-12-29 10:10:04 -06
Last Token Request Result	OK
Has Token	true
Next Token Request	not scheduled
Last Token Error	EDGE_AUTH_ERROR: 3, 54, 3ea

Basic troubleshooting steps

Before you start troubleshooting, check the Common sync issues to see if any of these issues apply to your sync problem.

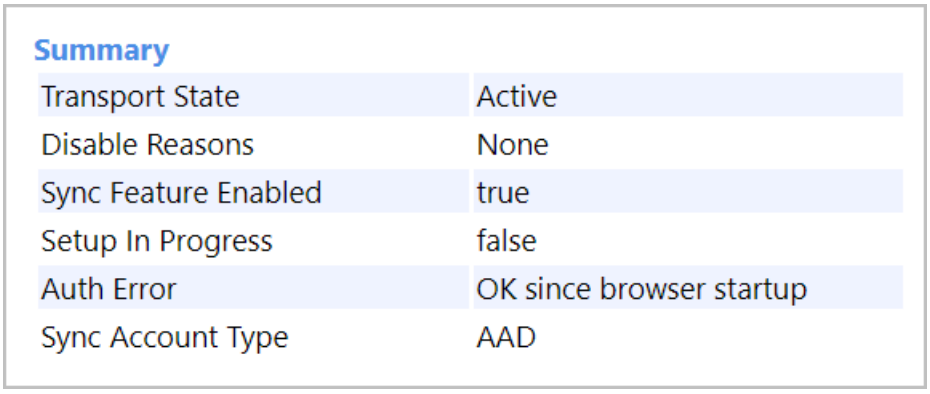
Use the following steps as a guide for troubleshooting a sync issue.

1. Sign in your Office 365 or Microsoft 365 admin portal and verify that your license is valid.
2. Sign in your Azure portal and verify that your Azure license is valid.
3. Sign out your account on all Microsoft Edge browsers on all the computers and/or mobile devices - not just the one you're using.

4. Make sure you're on the latest version of Microsoft Edge that supports all the sync features (at least 98.0.1108.43 (Official build) (64-bit)).

5. Sign back into your profile on Microsoft Edge. We recommend that you do a sync reset. For more information, see Perform a reset to fix a synchronization problem.

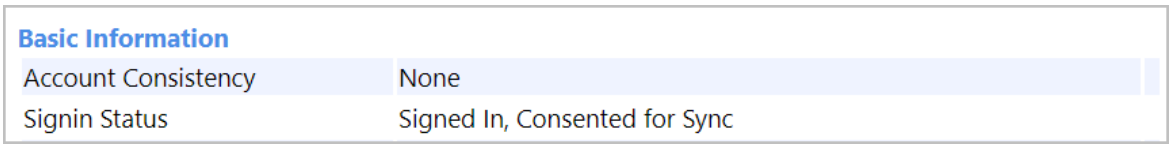
6. Verify that your account is enabled for syncing. On a new tab, go to: *edge://sync-internals/*. The Summary section, shown in the next screenshot shows that sync is enabled.



Summary	
Transport State	Active
Disable Reasons	None
Sync Feature Enabled	true
Setup In Progress	false
Auth Error	OK since browser startup
Sync Account Type	AAD

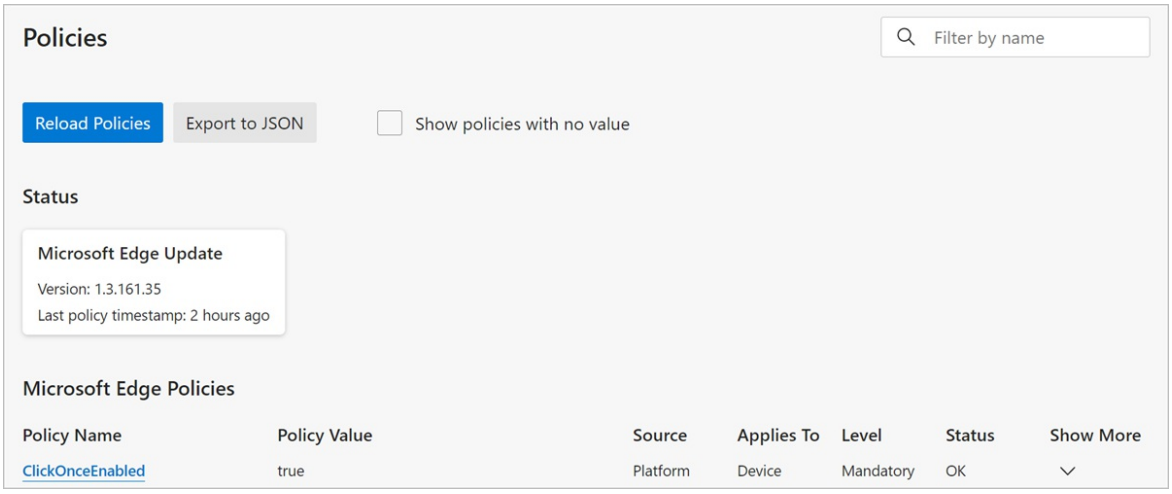
7. Verify that the device you're on is getting sync'ed. Go to *edge://sync-internals/* and select the **Sync Node Browser** tab. Open the **Device info** folder to see which devices are in the sync list.

8. Check your sign-in status. Go to *edge://signin-internals/*. The next screenshot shows the sign-in status for a user.



Basic Information	
Account Consistency	None
Signin Status	Signed In, Consented for Sync

9. Check to see if there are any policies that might prevent syncing. Go to *edge://policy/* to see the Policies page. The next screenshot shows an example of active policies for a signed in user. This page also shows Policy Precedence and Microsoft Edge Update Policies.



Common sync issues

Issue: Can't access Microsoft 365 or Azure Information Protection subscription

Do you have a previous Microsoft 365 or Azure Information Protection (AIP) subscription that expired and then replaced with a new subscription? If so, then the tenant ID has changed and the service data needs to be reset. See the instructions for resetting data in Issue: Cryptographer error encountered.

Issue: "Sync is not available for this account."

If this error is encountered for an Azure Active Directory account, or if DISABLED_BY_ADMIN appears in *edge://sync-internals*, follow the steps in the next procedure sequentially until the problem is fixed.

> **NOTE**
> Because the source of this error usually needs a configuration change in an Azure Active Directory tenant, these troubleshooting steps can only performed by a tenant admin.

1. Verify that the enterprise tenant has one of the supported subscriptions in Configure Microsoft Edge enterprise sync. To find out which subscription you have, see What subscription do I have?. If the tenant doesn't have a supported subscription, they can either purchase Azure Information Protection separately, or upgrade to one of the supported subscriptions.

2. If a supported subscription is available, verify that the tenant has Azure Information Protection (AIP). If you need to check AIP status and, if necessary, activate AIP, see these instructions: Activating the protection service from Azure Information Protection.

3. If step 2 shows that AIP is active but sync still doesn't work, turn on Enterprise State Roaming (ESR). If you need to enable ESR, see these instructions: Enable Enterprise State Roaming in Azure Active Directory.

   > **NOTE**
   > ESR doesn't need to stay on. You can turn off ESR if this step fixes the issue.

4. Confirm that Azure Information Protection isn't scoped via an onboarding policy. You can use the Get-AIPServiceOnboardingControlPolicy PowerShell cmdlet to see if scoping is enabled. Make sure the aIPService PowerShell monitor is installed. You can get it here: Install the AIPService PowerShell module for Azure Information Protection. The next two examples show an unscoped configuration and a configuration scoped to a specific security group.

   ```
   PS C:\Work\scripts\PowerShell> Get-AIPServiceOnboardingControlPolicy

   UseRmsUserLicense SecurityGroupObjectId                Scope
   ----------------- ---------------------                -----
               False
   ```

   ```
   PS C:\Work\scripts\PowerShell> Get-AIPServiceOnboardingControlPolicy

   UseRmsUserLicense SecurityGroupObjectId                Scope
   ----------------- ---------------------                -----
               False f1488a05-8196-40a6-9483-524948b90282   All
   ```

   If scoping is enabled, the affected user should either be added to the security group for the scope, or the scope should be removed. Scoping can be removed with the Set-AIPServiceOnboardingControlPolicy PowerShell applet.

5. Confirm that the IPCv3Service is turned on in the tenant. The Get-AIPServiceConfiguration PowerShell cmdlet shows the status of the service.

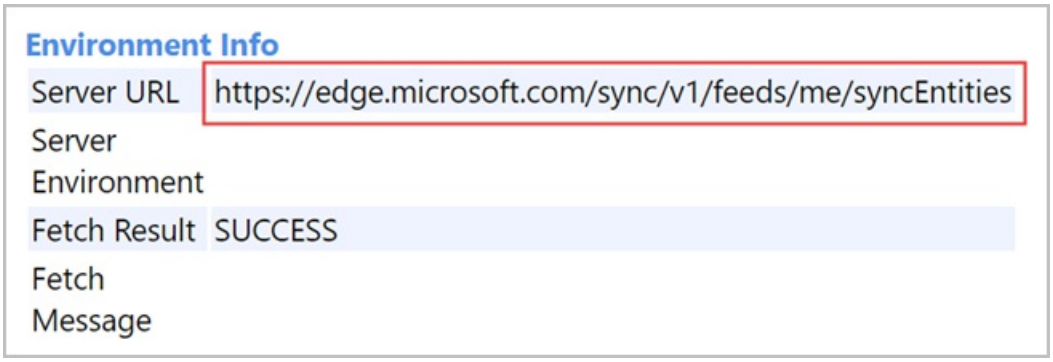
6. If the issue isn't fixed, contact Microsoft Edge support.

Issue: Stuck at "Setting up sync..." or "Couldn't connect to the sync server. Retrying..."

1. Try to sign out and then sign in.
2. Go to *edge://sync-internals*. If the following error appears under the **Type info** section, skip to the Cryptographer error encountered issue.

```
"Error:GenerateCryptoErrorsForTypes@../../components/sync/driver/data_type_manager_impl.cc:42,
cryptographer error was encountered"
```

3. Try pinging the server endpoint. The server endpoint for a client is available in *edge://sync-internals*. The next screenshot shows endpoint information under **Environment Info**.



4. If the server endpoint is empty, or if server can't be pinged because there's a firewall in the environment, confirm that the necessary service endpoints are available to the client device.

   - Microsoft Edge sync service endpoints:
     - `https://edge-enterprise.activity.windows.com`
     - `https://edge.activity.windows.com`
   - Azure Information Protection endpoints:
     - `https://api.aadrm.com` (for most tenants)
     - `https://api.aadrm.de` (for tenants in Germany)
     - `https://api.aadrm.cn` (for tenants in China)
   - Enterprise Firewall Configurations to Support WNS Traffic.

5. If the issue still isn't fixed, contact Microsoft Edge support.

Issue: Cryptographer error encountered

This error is visible under **Type info** in *edge://sync-internals* and might mean that the user's service side data needs to be reset. The next example shows a cryptography error message:

```
"Error:GenerateCryptoErrorsForTypes@../../components/sync/driver/data_type_manager_impl.cc:42, cryptographer
error was encountered".
```

Use the following steps to fix this issue:

1. Restart Microsoft Edge and go to *edge://sync-internals*. Look at the **AAD Account Key Status** section to see if any of the following messages are present:
   - Last MIP Result = "Success": This error means server data might be encrypted with a lost key. A data reset is needed to resume sync.

- Last MIP Result = "No permissions": It's possibly caused by an Azure AD change or tenant subscription changes. A data reset is needed to resume sync.
- Other errors may mean there's a server configuration issue.

2. If a data reset is needed, see Reset Microsoft Edge data in the cloud.

Issue: "Sync has been turned off by your administrator."

Make sure that the SyncDisabled policy isn't set.

See also

- Microsoft Edge Enterprise Sync
- Microsoft Edge enterprise sync FAQ
- Microsoft Edge and Enterprise State Roaming
- Microsoft Edge Enterprise landing page

Microsoft Edge enterprise sync FAQ

11/1/2022 • 2 minutes to read • Edit Online

This article answers frequently asked questions about enterprise sync for Microsoft Edge version 77 or later.

Security and Server/Data compliance

Is the synced data encrypted?

Yes, the data is encrypted in transport using TLS 1.2 or greater. All data types are additionally encrypted at rest in Microsoft's service using AES128. All data types except the data used for open tab and history sync are additionally encrypted before leaving the user's device with keys managed via the Azure Information Protection policy.

Why isn't there more client-side encryption on open tab and history data?

To reduce resource utilization on end-user devices, history data is generated server-side based on open tab roaming data. This process wouldn't be possible with client-side encryption of this data. To disable open tab and history sync, apply the SavingBrowserHistoryDisabled or SyncTypesListDisabled policies.

Can tenant admins bring their own key?

Yes, throughAzure Information Protection.

Where is Microsoft Edge sync data stored?

Synced data for Azure AD accounts is stored on secure servers according to the tenant ID. For example, the data for a tenant that is registered in the United States is stored in servers geo-located for that region and uses the same storage solution as Office applications.

Does the data ever leave Microsoft's cloud, aside from syncing to Microsoft Edge?

No.

What terms of service does enterprise sync fall under?

Terms of service for Microsoft Edge sync fall under the Microsoft software license viewable in Microsoft Edge at*edge://terms*. Your Azure AD subscription and terms of service ultimately fall under Microsoft's Online Service Terms.

Does Microsoft Edge support Government Community Cloud (GCC) High compliance?

Not today. For customers in the GCC High cloud, Microsoft Edge sync is disabled.

Applying Sync

Why isn't Microsoft Edge sync supported in all Microsoft 365 subscriptions?

Enterprise sync depends on Azure Information Protection, which isn't available for all Microsoft 365 subscriptions.

Is Microsoft Edge sync based on Enterprise State Roaming?

No. ESR can be used to enable sync, but Microsoft Edge sync isn't a part of ESR. For more information, see Microsoft Edge Sync and Microsoft Edge and Enterprise State Roaming.

Will Microsoft Edge ever support syncing between Microsoft Edge and IE?

There are no plans to support this syncing. If you still need IE in your environment to support legacy apps, consider our new IE mode.

Will Microsoft Edge sync with Microsoft Edge Legacy?

No, it won't. We believe connecting these two ecosystems will lead to compromises in the reliability of sync in the Microsoft Edge. We'll ensure that existing data is migrated to the Microsoft Edge. Users will also be able to import data from browser of their choice, which also means that Microsoft Edge won't have a way to sync with IE.

Managing Sync

Is it possible to stop my users from syncing with a personal tenant?

Not directly, but you can determine which profiles can sign on to Microsoft Edge using the RestrictSigninToPattern policy.

Is it possible to prevent sign-in and sync with an enterprise account on an unmanaged/non-compliant device?

Currently it's not possible to prevent Azure AD sign-in to Microsoft Edge on unmanaged devices without disrupting your other Conditional Access (CA) protected applications. However, enterprise sync can be blocked on such devices by adding the "Microsoft Azure Information Protection" app to the CA policy.

See also

- Microsoft Edge Enterprise Sync
- Microsoft Edge and Enterprise State Roaming
- Microsoft Edge Enterprise landing page

On-premises sync for Active Directory (AD) users

11/1/2022 • 3 minutes to read • Edit Online

This article explains how Active Directory (AD) users can roam Microsoft Edge favorites and settings between computers without connecting to Microsoft cloud services.

> **NOTE**
> This article applies to Microsoft Edge version 85 or later.

Introduction

Syncing user data in Microsoft Edge normally requires either a Microsoft Account or an Azure Active Directory (Azure AD) account, and a connection to Microsoft cloud services. With on-premises sync, Microsoft Edge saves an Active Directory user's favorites and settings to a file that can be moved between different computers. On-premises sync doesn't interfere with cloud syncing for those profiles that allow it.

How it works

Microsoft Edge allows profiles to be associated with Active Directory (AD) accounts, which can't be used with cloud sync. When on-premises sync is enabled, the data from the AD profile is saved to a file named profile.pb. By default, this file is stored in *%APPDATA%/Microsoft/Edge*. After this file is written, it can be moved between different computers, and user data will be read and written on each computer. Microsoft Edge only reads and writes from this file; it's the admin's responsibility to ensure that the file is moved as needed.

Use on-premises sync

To use on-premises sync, you have to enable it, associate a profile with an AD account, and optionally, change the location of the user data.

Enable on-premises sync

To enable on-premises sync in Microsoft Edge, configure the RoamingProfileSupportEnabled policy.

Ensure that a profile is associated with an Active Directory account

On-premises sync only works with the profile associated with an Active Directory (AD) account. If this profile doesn't exist, on-premises sync won't work. To ensure that users sign on with an AD account, configure the ConfigureOnPremisesAccountAutoSignIn policy. For on-premises sync, Microsoft Edge only relies on AD to establish an identity for the user data, and there's no direct relationship between how Microsoft Edge reads and writes on-premises data to how the admin has configured roaming for an AD user.

Change the location of the user data (optional)

By default, the user data is stored in a filed named **profile.pb** in *%APPDATA%/Microsoft/Edge*. To change the location of this file, configure the RoamingProfileLocation policy.

Changes in the user experience when on-premises sync is enabled

When on-premises sync is enabled, users won't be asked to enable sync. In addition, users can't turn off sync in Sync settings, and they can't turn on sync types that aren't supported by on-premises sync.

On-premises sync usage notes

Running cloud sync and on-premises sync on the same computer

On-premises sync doesn't interfere with cloud sync. If Microsoft Edge has multiple Microsoft Account or Azure Active Directory profiles that sync to the cloud, these profiles will continue to sync while on-premises sync is enabled.

Running Microsoft Edge on more than one computer at a time isn't recommended

Because on-premises sync works by moving a user data file between computers, on-premises sync doesn't sync changes between simultaneous sessions. For this reason, on-premises sync works best when used on one computer at a time. If there are simultaneous on-premises sessions running, data on any of the computers may be unexpectedly overwritten by data from another computer the next time you start a browser session.

> **NOTE**
> Microsoft Edge locks the **profile.pb** file when on-premises sync is enabled. If folder redirection is used to share a single **profile.pb** file between different computers, then only one instance of Microsoft Edge that uses the shared file can be started.

Using other sync policies with on-premises sync

The SyncTypesListDisabled policy can be used to selectively disable either favorites or settings sync if desired. The SyncDisabled policy has no impact on on-premises sync.

See also

- Microsoft Edge Enterprise landing page
- Microsoft Edge and Enterprise State Roaming
- Microsoft Edge Enterprise Sync

PDF reader in Microsoft Edge

11/1/2022 • 8 minutes to read • Edit Online

PDF files make up a large part of our day-to-day lives. They come in the form of contracts and agreements, newsletters, forms, research articles, resumes, and so on. These files highlight the need for a reliable, secure, and powerful PDF reader that can be adopted by Enterprises.

Microsoft Edge comes with a built-in PDF reader that lets you open your local pdf files, online pdf files, or pdf files embedded in web pages. You can annotate these files with ink and highlighting. This PDF reader gives users a single application to meet web page and PDF document needs. The Microsoft Edge PDF reader is a secure and reliable application that works across the Windows and macOS desktop platforms.

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

Prerequisites, support, and constraints

The following table shows which channels and versions of Microsoft Edge support each PDF reader feature.

FEATURE	STABLE CHANNEL VERSION
View and print local, online, and embedded PDF files	79.0.309.71
Basic form filling (JavaScript forms aren't supported)	79.0.309.71
Table of contents	86.0.622.38
Page view	88.0.705.50
Caret mode browsing	87.0.664.41
Inking	80.0.361.48
Ink customization	83.0.478.54
Highlight	81.0.416.53
Text notes	88.0.705.50
Read aloud	84.0.522.63
View Microsoft Purview Information Protection protected files in the same business tenant	Windows support in 80.0.361.48 Mac support in 81.0.416.53
View Microsoft Purview Information Protection protected files across business tenants	91.0.864.37

FEATURE	STABLE CHANNEL VERSION
View Information Rights Management (IRM) protected files	83.0.478.37

Constraints

Note the following constraints for the current PDF reader:

- XML Forms Architecture (XFA), is a legacy format of forms that isn't supported in Microsoft Edge.
- Documentation related to Accessibility scenarios that currently aren't supported can be found on the Microsoft Accessibility Conformance Reports blog.

Features

The PDF reader, built into Microsoft Edge, comes with the basic reading and navigation features, as Zoom, Rotate, Fit to page/width, jump to page, and search, among others. They can be accessed through a pin-able toolbar at the top of PDF content. This section gives an overview of some important functions. The next screenshot shows the PDF reader toolbar.

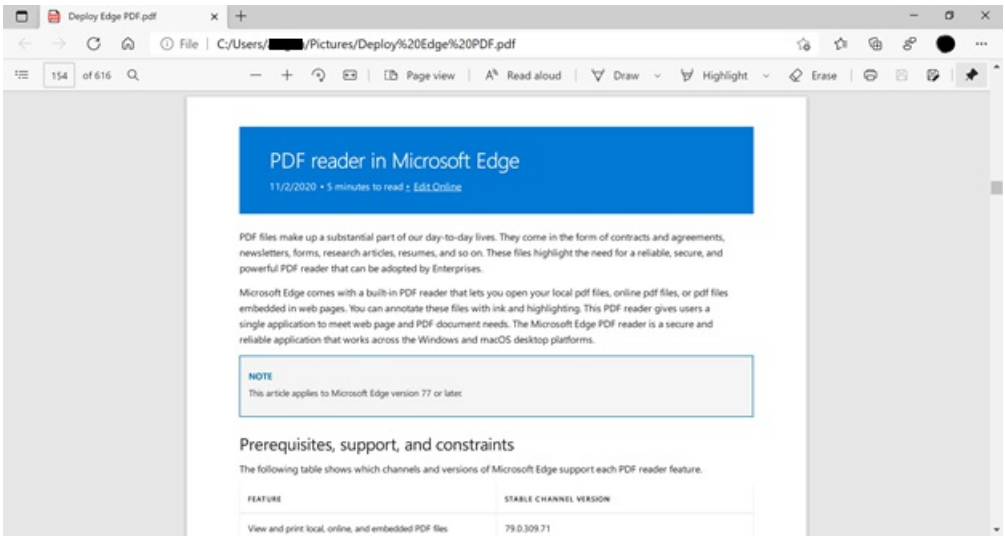
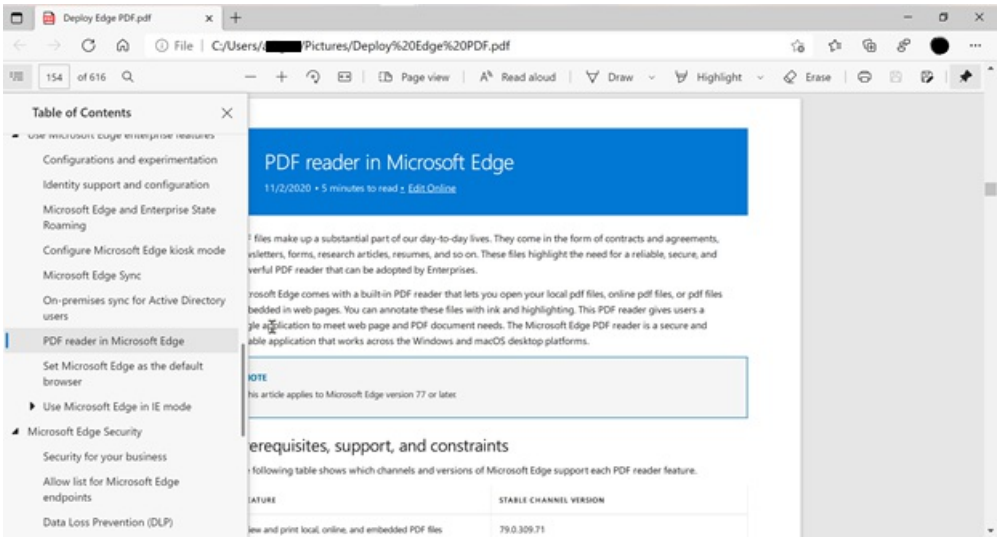

Deploy Edge PDF.pdf
C:/Users/[redacted]/Pictures/Deploy%20Edge%20PDF.pdf
154 of 616
Page view
Read aloud
Draw
Highlight
Erase
PDF reader in Microsoft Edge
11/2/2020 • 5 minutes to read • Edit Online
PDF files make up a substantial part of our day-to-day lives. They come in the form of contracts and agreements, newsletters, forms, research articles, resumes, and so on. These files highlight the need for a reliable, secure, and powerful PDF reader that can be adopted by Enterprises.
Microsoft Edge comes with a built-in PDF reader that lets you open your local pdf files, online pdf files, or pdf files embedded in web pages. You can annotate these files with ink and highlighting. This PDF reader gives users a single application to meet web page and PDF document needs. The Microsoft Edge PDF reader is a secure and reliable application that works across the Windows and macOS desktop platforms.
NOTE
This article applies to Microsoft Edge version 77 or later.
Prerequisites, support, and constraints
The following table shows which channels and versions of Microsoft Edge support each PDF reader feature.
FEATURE
STABLE CHANNEL VERSION
View and print local, online, and embedded PDF files
79.0.309.71

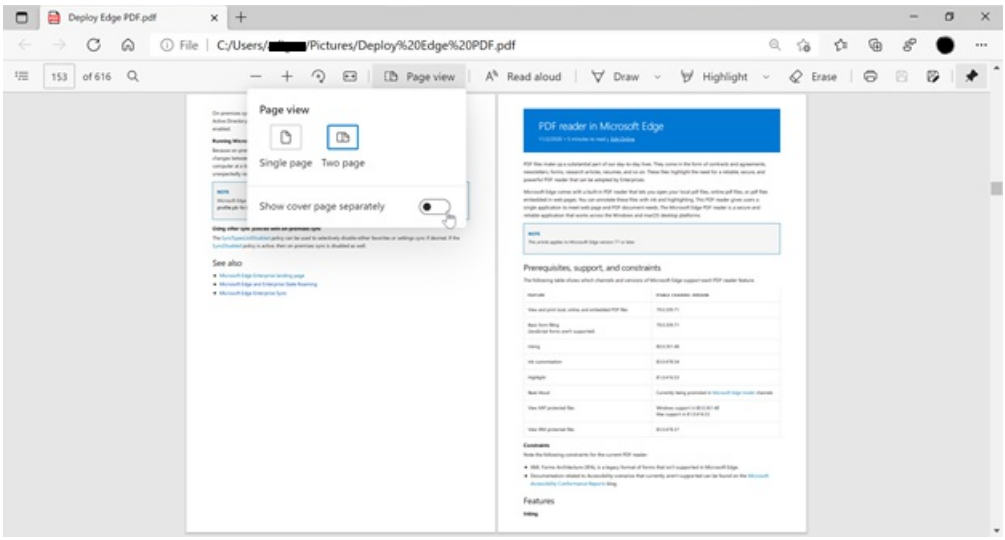
Table of contents

Table of contents lets users easily navigate through PDF documents that have a table of contents. When a user clicks the Table of contents icon, a navigation pane that shows a list of the labeled sections and subsections in the PDF document is shown. The user can then click any of the labels in the pane to navigate to that section of the document. The pane stays open for as long as needed and can be closed when the user wants to go back to reading the document. The next screenshot shows the navigation pane for an open document.



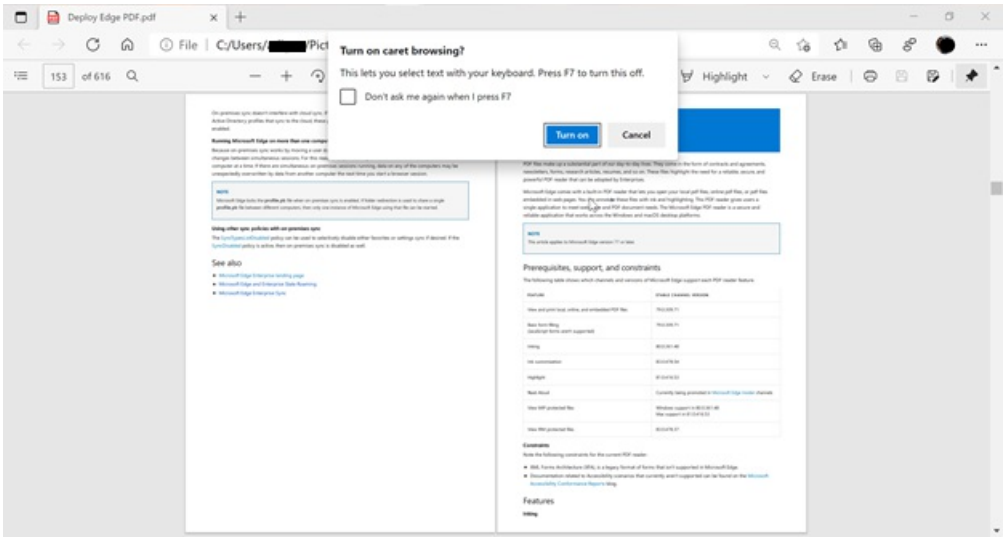
Page view

Microsoft Edge supports different views for PDF documents in our Dev and Canary channels. Users can change the layout of a document from a single page view to two pages that are displayed side by side. To change how the PDF document is being viewed, users can click the Page View button in the PDF toolbar and then choose either view they want to use. The two page view is shown in the next screenshot.



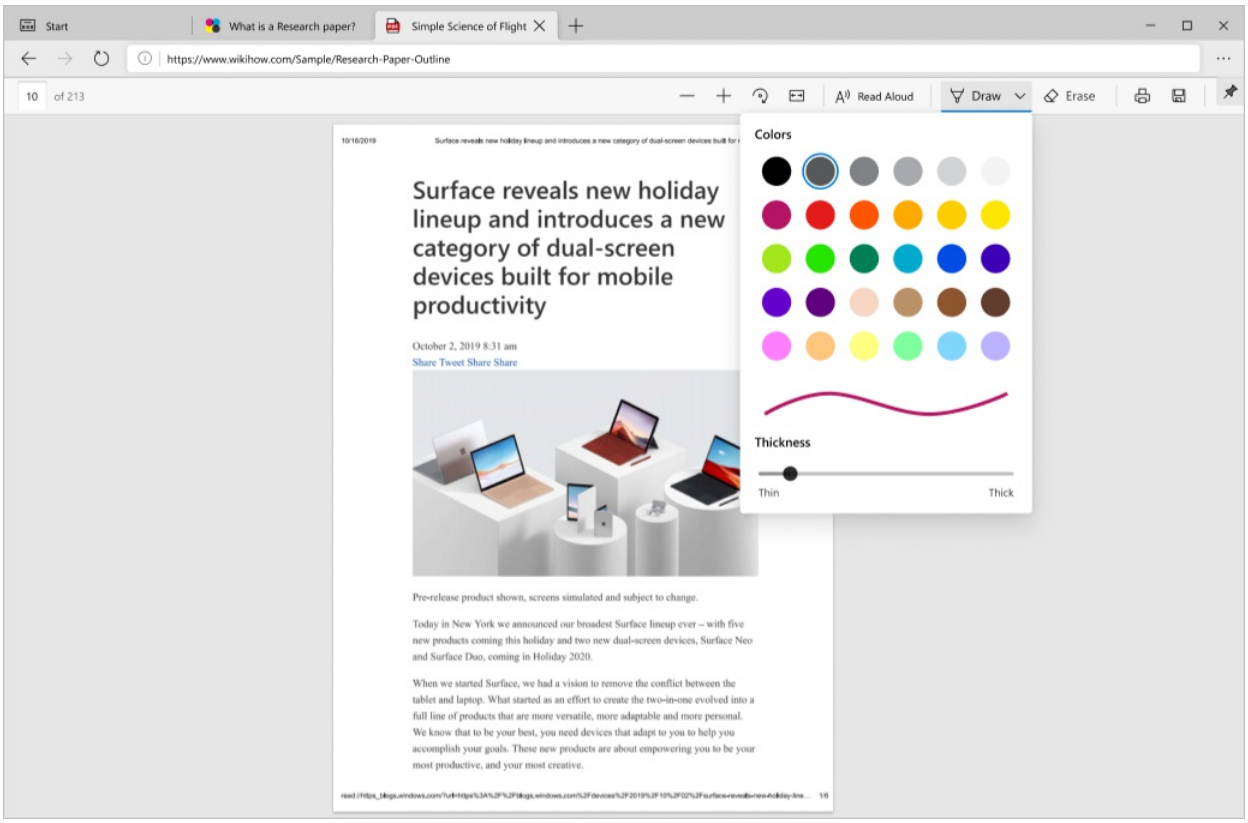
Caret mode browsing

Caret browsing is available for PDF files opened in Microsoft Edge, which means that users can interact with PDF files using the keyboard. If a user presses the F7 key anywhere in the browser, they're asked if caret browsing should be turned on. If enabled, caret browsing is available for any content opened in the browser, be it PDF files or web pages. When a user presses F7 again, caret browsing is turned off. When caret browsing is active and the focus is on the content, users will see a blinking cursor in the PDF file. The caret can also be used to navigate through the file, or to select text by pressing Shift while moving the cursor. This ability lets users easily create elements as highlights, or interact with elements as links, form fields with the keyboard. The next screenshot shows the popup menu for turning on Caret mode browsing.



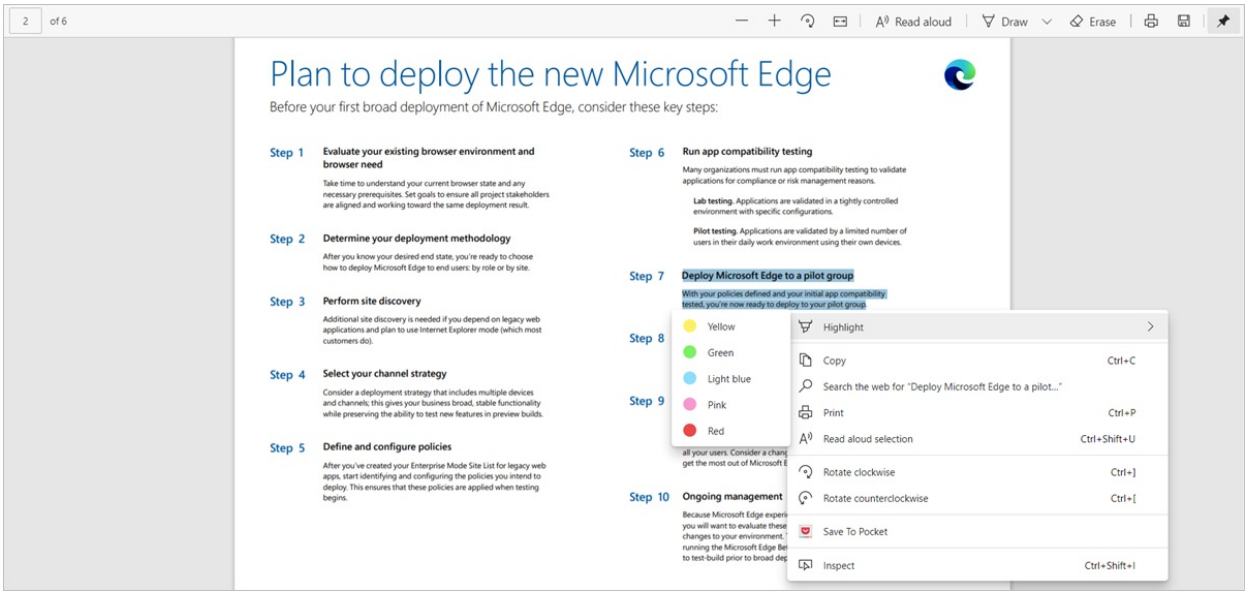
Inking

Inking on PDF files comes in handy to take quick notes for easy reference, sign, or fill out PDF forms. This capability is now available in Microsoft Edge. In addition to inking PDF files as needed, you can use color and stroke width to bring attention to different parts of the PDF file. The next screenshot shows how a user can add inking to a pdf page.


Start
What is a Research paper?
Simple Science of Flight
https://www.wikihow.com/Sample/Research-Paper-Outline
10 of 213
Read Aloud
Draw
Erase
Colors
Thickness
Thin
Thick
Surface reveals new holiday lineup and introduces a new category of dual-screen devices built for mobile productivity
October 2, 2019 8:31 am
Share Tweet Share Share
Pre-release product shown, screens simulated and subject to change.
Today in New York we announced our broadest Surface lineup ever – with five new products coming this holiday and two new dual-screen devices, Surface Neo and Surface Duo, coming in Holiday 2020.
When we started Surface, we had a vision to remove the conflict between the tablet and laptop. What started as an effort to create the two-in-one evolved into a full line of products that are more versatile, more adaptable and more personal. We know that to be your best, you need devices that adapt to you to help you accomplish your goals. These new products are about empowering you to be your most productive, and your most creative.

Highlight

PDF reader in Microsoft Edge comes with support for adding and editing highlights. To create a highlight, the user simply needs to select the text, right-click on it, select highlights in the menu and choose the desired color. Highlights can also be created using a pen, or keyboard. The next screenshot shows the highlight options that are available.



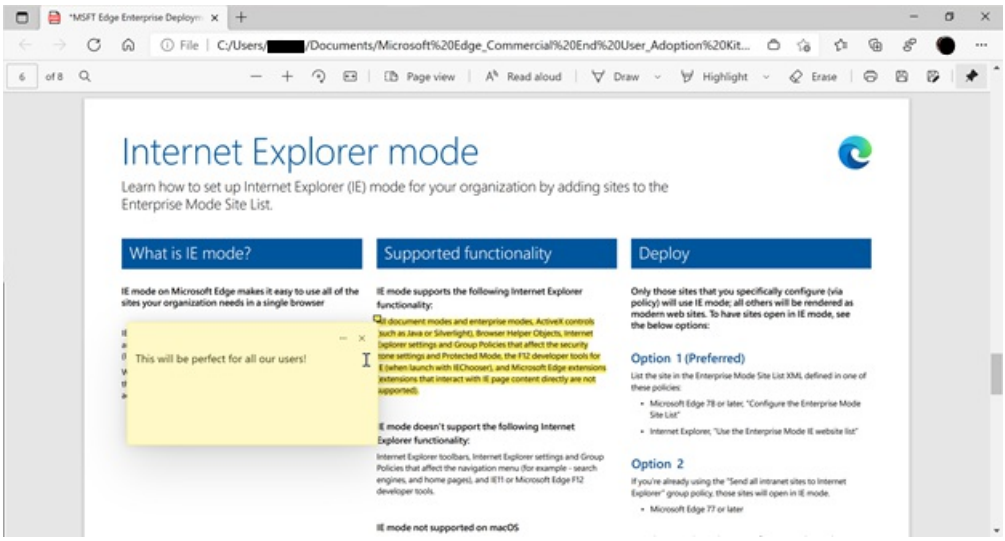
Text notes

While reading a PDF file, text notes can be added to text in the file to jot down thoughts for easy reference later.

Users can add a note by selecting the piece of text they wish to add a note for and invoking the right-click context menu. Selecting the **Add Comment** option in the menu will open a text box where users can add their comments. They can type the comment and then click the check mark to save the comment.

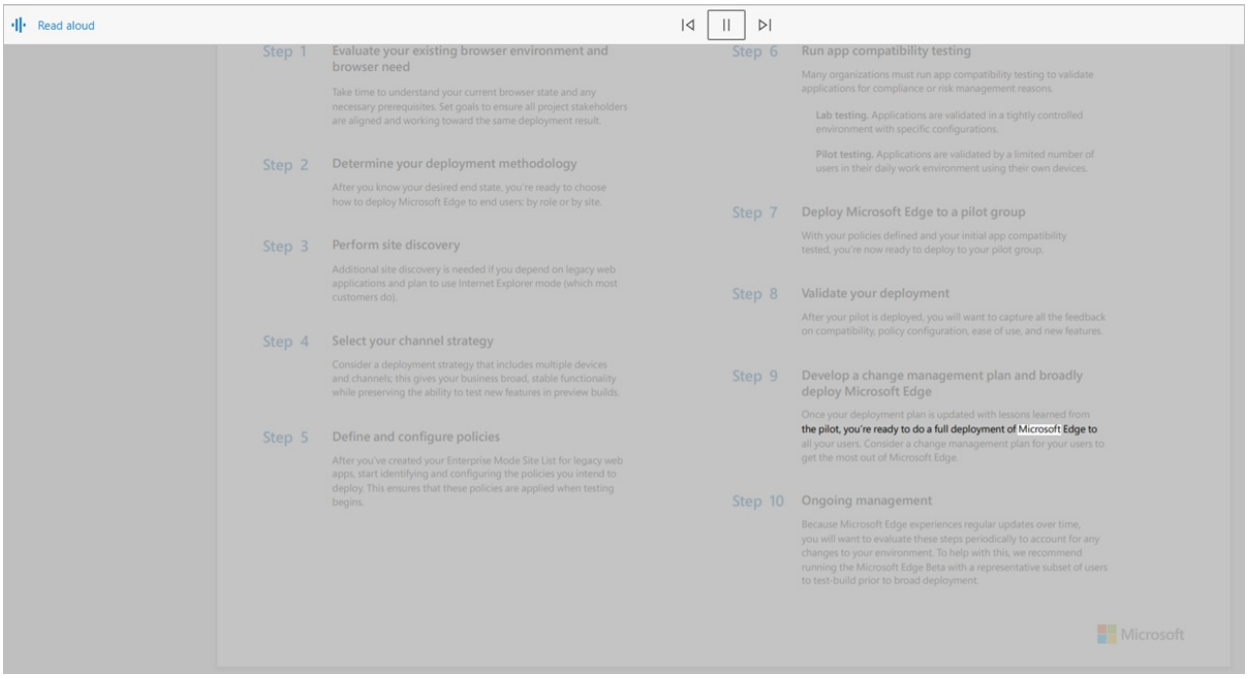
After a note is added, the selected text will be highlighted, and a comment icon will appear to indicate the comment. Users can hover over that icon to preview the comment or click on it to open and edit the note.

The next screenshot shows a note getting added to highlighted text.


Internet Explorer mode
Learn how to set up Internet Explorer (IE) mode for your organization by adding sites to the Enterprise Mode Site List.
What is IE mode?
Supported functionality
Deploy
IE mode on Microsoft Edge makes it easy to use all of the sites your organization needs in a single browser
This will be perfect for all our users!
IE mode supports the following Internet Explorer functionality:
IE mode doesn't support the following Internet Explorer functionality:
Internet Explorer toolbars, Internet Explorer settings and Group Policies that affect the navigation menu (for example - search engines, and home pages), and IE11 or Microsoft Edge F12 developer tools.
IE mode not supported on macOS
Only those sites that you specifically configure (via policy) will use IE mode; all others will be rendered as modern web sites. To have sites open in IE mode, see the below options:
Option 1 (Preferred)
List the site in the Enterprise Mode Site List XML defined in one of these policies:
Microsoft Edge 78 or later, "Configure the Enterprise Mode Site List"
Internet Explorer, "Use the Enterprise Mode IE website list"
Option 2
If you're already using the "Send all intranet sites to Internet Explorer" group policy, those sites will open in IE mode.
Microsoft Edge 77 or later

Read aloud

Read aloud for PDF adds the convenience of listening to PDF content while carrying out other tasks that may be important to users. It also helps auditory learners focus on the content, which makes learning much easier. The next screenshot shows a Read aloud example. The highlighting shows the text that is currently being read.

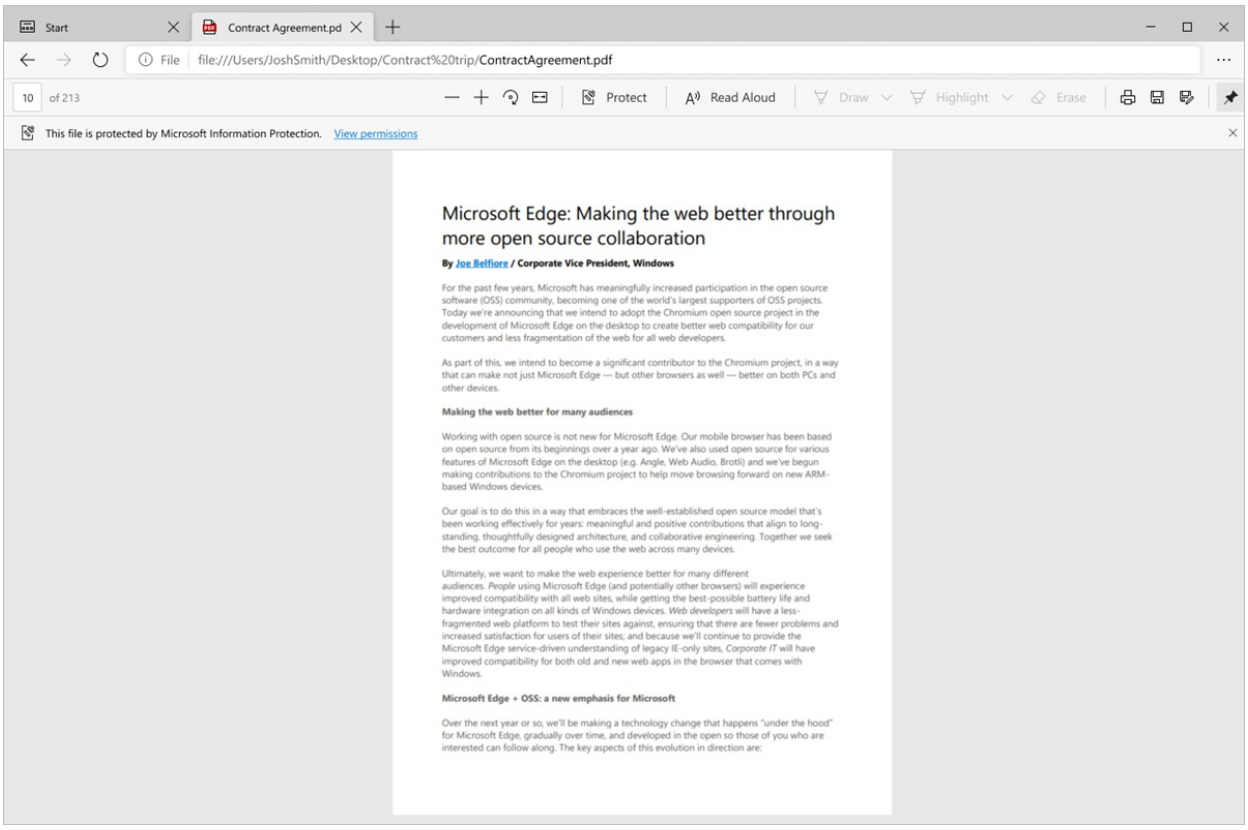

Read aloud
Step 1 Evaluate your existing browser environment and browser need
Step 2 Determine your deployment methodology
Step 3 Perform site discovery
Step 4 Select your channel strategy
Step 5 Define and configure policies
Step 6 Run app compatibility testing
Step 7 Deploy Microsoft Edge to a pilot group
Step 8 Validate your deployment
Step 9 Develop a change management plan and broadly deploy Microsoft Edge
Step 10 Ongoing management
Microsoft

Protected PDFs

Microsoft Purview Information Protection enables users to collaborate with others securely, while adhering to your organization's compliance policies. After a file is protected, the actions users can take on it are determined by the permissions assigned to them.

> **IMPORTANT**
>
> A license is required for MIP. For more information, see this Microsoft 365 licensing guidance.

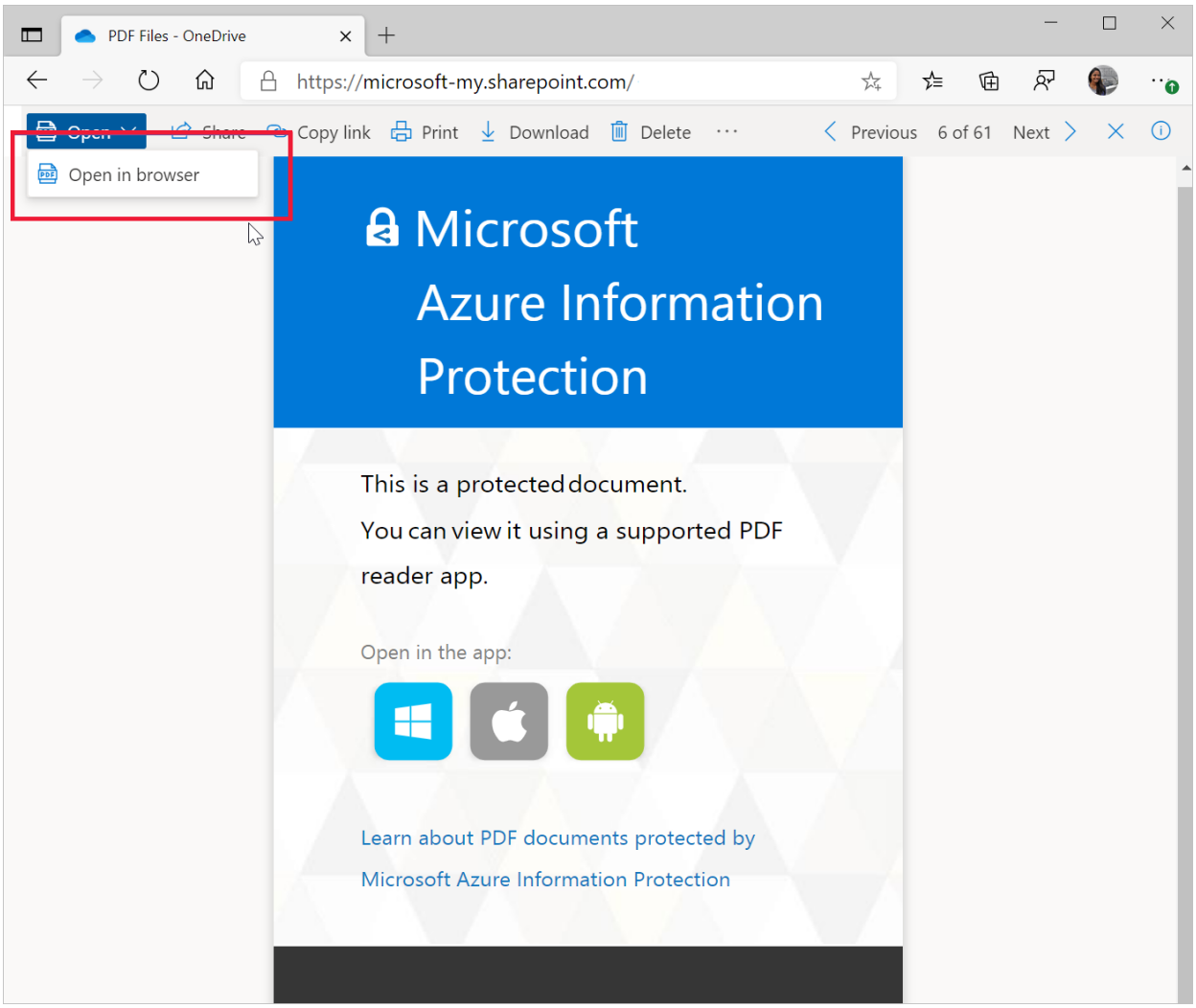
These files can be opened directly in the browser, without the need to download any other software, or install any add-in. This capability integrates the security provided by MIP directly into the browser, providing a seamless workflow. You can view MIP Protected files across business tenants. Viewing files using consumer identities currently is not supported.


Start
Contract Agreement.pd
File
file:///Users/JoshSmith/Desktop/Contract%20trip/ContractAgreement.pdf
10
of 213
Protect
Read Aloud
Draw
Highlight
Erase
This file is protected by Microsoft Information Protection.
View permissions
Microsoft Edge: Making the web better through more open source collaboration
By Joe Belfiore / Corporate Vice President, Windows
For the past few years, Microsoft has meaningfully increased participation in the open source software (OSS) community, becoming one of the world's largest supporters of OSS projects. Today we're announcing that we intend to adopt the Chromium open source project in the development of Microsoft Edge on the desktop to create better web compatibility for our customers and less fragmentation of the web for all web developers.
As part of this, we intend to become a significant contributor to the Chromium project, in a way that can make not just Microsoft Edge — but other browsers as well — better on both PCs and other devices.
Making the web better for many audiences
Working with open source is not new for Microsoft Edge. Our mobile browser has been based on open source from its beginnings over a year ago. We've also used open source for various features of Microsoft Edge on the desktop (e.g. Angle, Web Audio, Brotli) and we've begun making contributions to the Chromium project to help move browsing forward on new ARM-based Windows devices.
Our goal is to do this in a way that embraces the well-established open source model that's been working effectively for years: meaningful and positive contributions that align to long-standing, thoughtfully designed architecture, and collaborative engineering. Together we seek the best outcome for all people who use the web across many devices.
Ultimately, we want to make the web experience better for many different audiences. People using Microsoft Edge (and potentially other browsers) will experience improved compatibility with all web sites, while getting the best-possible battery life and hardware integration on all kinds of Windows devices. Web developers will have a less-fragmented web platform to test their sites against, ensuring that there are fewer problems and increased satisfaction for users of their sites; and because we'll continue to provide the Microsoft Edge service-driven understanding of legacy IE-only sites, Corporate IT will have improved compatibility for both old and new web apps in the browser that comes with Windows.
Microsoft Edge + OSS: a new emphasis for Microsoft
Over the next year or so, we'll be making a technology change that happens "under the hood" for Microsoft Edge, gradually over time, and developed in the open so those of you who are interested can follow along. The key aspects of this evolution in direction are:

In addition to MIP protected files, PDF files in Information Rights Management (IRM) protected SharePoint libraries can also be opened natively in the browser.

With Microsoft Edge, users can view MIP protected files saved locally, or in the cloud. If saved locally, the file can be opened directly in the browser. If the file is opened from a cloud service as SharePoint, the user may need to use the "Open in browser" option.

If the profile that the user is logged into Microsoft Edge with has at least view permissions to the file, the file will open in Microsoft Edge.



View and validate certificate-based digital signatures

In this digital world, it becomes important to establish the authenticity and ownership of the content in the document. Certificate-based digital signatures are commonly used in PDF documents to ensure that the content in the document is the same as what the author intended it to be, and has not been changed. With Microsoft Edge, you can view and validate certificate digital signatures in PDFs.

We're actively working on improving the support to address more scenarios, and are looking forward for feedback about the same.

Accessibility

The PDF reader comes with support for Keyboard accessibility, High contrast mode, and screen reader support across Windows and macOS devices.

Keyboard Accessibility

Users can use navigate to different parts of the document that a user can interact with, such as form fields and highlights, using the keyboard. Users can also use Caret mode to navigate and interact with the PDF files using the keyboard.

High contrast mode

PDF reader will use the settings defined at the operating system level to render PDF content in high contrast mode.

Screen reader support

Users can navigate through and read PDF files using screen readers on Windows and Mac computers.

Security and reliability

Security is among the most important tenets for any organization. PDF reader security is an integral part of the Microsoft Edge security design. Two of the most important security features From a PDF reader perspective, two important security features are process isolation and Microsoft Defender Application Guard (Application Guard).

- Process isolation. PDFs opened from different web sites are completely process isolated. The browser doesn't have to communicate with any websites, or PDF files opened from another source. PDF browsing is secure from any attacks that plan to use compromised PDFs as an attack surface.
- Application Guard. With Application Guard, admins can set a list of sites that are trusted by their organization. If users open any other sites, they are opened in a separate Application Guard window that runs in its own container. The container helps protect the corporate network and any data on user's computer from being compromised.

  This protection also applies to any online PDF files that are viewed. Further, any PDF files that are downloaded from an Application Guard window are stored, and when needed, re-opened in the container. This helps keeps your environment secure not just when the file is downloaded, but through its whole lifecycle. For more information, see Application Guard.

Reliability

Because Microsoft Edge is Chromium-based, users can expect the same level of reliability that they're used to seeing in other Chromium-based browsers.

Deploy and update PDF reader

The PDF reader gets deployed and updated with the rest of the Microsoft Edge browser. To learn more about deploying Microsoft Edge, watch the Deploy Microsoft Edge to hundreds or thousands of devices video. You can also find more deployment information on the Microsoft Edge documentation landing page.

> **TIP**
> You can make Microsoft Edge the default PDF reader for your organization. To do this, follow these steps.

Roadmap and feedback

The roadmap for PDF reader in Microsoft Edge is available here.

We're actively looking at feedback from you about the features you find important. Feel free to send us feedback through the Microsoft Edge Insider forum.

See also

- Microsoft Edge Enterprise landing page
- Microsoft 365 Roadmap
- Video: Microsoft Edge enterprise grade PDF reader

Set Microsoft Edge as the default browser

11/1/2022 • 3 minutes to read • Edit Online

This article explains how you can set Microsoft Edge as the default browser on Windows and macOS.

> **NOTE**
> This article applies to Microsoft Edge version 77 or later on Windows 8 and Windows 10. For Windows 7 and macOS, see the Set Microsoft Edge as default browser policy.

Introduction

You can use the **Set a default associations configuration file** Group Policy or the DefaultAssociationsConfiguration Mobile Device Management setting to set Microsoft Edge as the default browser for your organization.

To set Microsoft Edge Stable as the default browser for html files, http/https links, and PDF files use the following application association file example:

```
<?xml version="1.0" encoding="UTF-8"?>
<DefaultAssociations>
  <Association ApplicationName="Microsoft Edge" ProgId="MSEdgeHTM" Identifier=".html"/>
  <Association ApplicationName="Microsoft Edge" ProgId="MSEdgeHTM" Identifier=".htm"/>
  <Association ApplicationName="Microsoft Edge" ProgId="MSEdgeHTM" Identifier="http"/>
  <Association ApplicationName="Microsoft Edge" ProgId="MSEdgeHTM" Identifier="https"/>
  <Association ApplicationName="Microsoft Edge" ProgId="MSEdgePDF" Identifier=".pdf"/>
</DefaultAssociations>
```

> **NOTE**
> To set Microsoft Edge Beta as the default browser, set **ApplicationName** to "Microsoft Edge Beta" and **ProgId** to "MSEdgeBHTML". To set Microsoft Edge Dev as the default browser, set **ApplicationName** to "Microsoft Edge Dev" and **ProgId** to "MSEdgeDHTML".

> **NOTE**
> The default file associations aren't applied if Microsoft Edge isn't installed on the target device. In this scenario, users are prompted to select their default application when they open a link or a htm/html file.

Set Microsoft Edge as the default browser on domain-joined devices

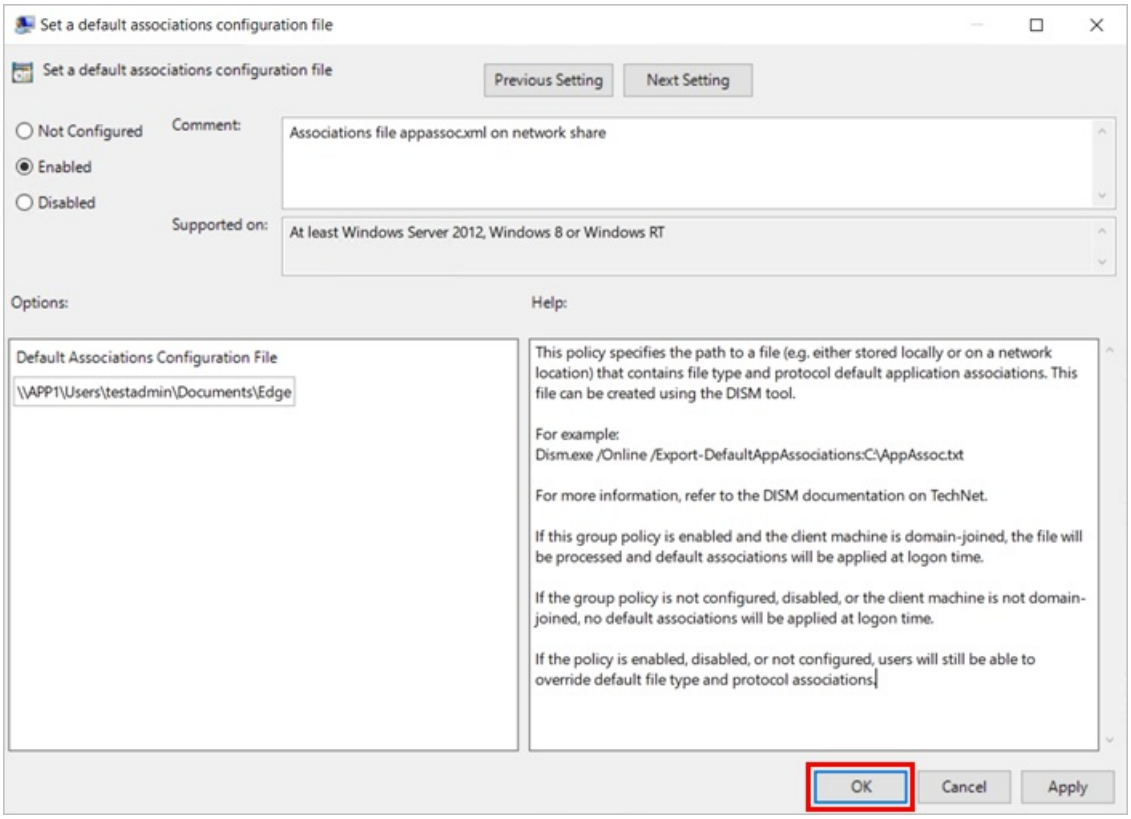
You can set Microsoft Edge as the default browser on domain-joined devices by configuring the **Set a default associations configuration file** group policy. Turning this group policy on requires you to create and store a default associations configuration file. This file is stored locally or on a network share. For more information about creating this file, see Export or Import Default Application Associations.

To configure the group policy for a default file type and protocol associations configuration file:

1. Open the Group Policy editor and go to the **Computer Configuration\Administrative Templates\Windows Components\File Explorer**.

2. Select **Set a default associations configuration file**.
3. Click **policy setting**, and then click **Enabled**.
4. Under **Options:**, type the location to your default associations configuration file.
5. Click **OK** to save the policy settings.

The example in the next screenshot shows an associations file named *appassoc.xml* on a network share that is accessible from the target device.


Set a default associations configuration file
Set a default associations configuration file
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Associations file appassoc.xml on network share
Supported on:
At least Windows Server 2012, Windows 8 or Windows RT
Options:
Help:
Default Associations Configuration File
\\APP1\Users\testadmin\Documents\Edge
This policy specifies the path to a file (e.g. either stored locally or on a network location) that contains file type and protocol default application associations. This file can be created using the DISM tool.
For example:
Dism.exe /Online /Export-DefaultAppAssociations:C:\AppAssoc.txt
For more information, refer to the DISM documentation on TechNet.
If this group policy is enabled and the client machine is domain-joined, the file will be processed and default associations will be applied at logon time.
If the group policy is not configured, disabled, or the client machine is not domain-joined, no default associations will be applied at logon time.
If the policy is enabled, disabled, or not configured, users will still be able to override default file type and protocol associations.
OK
Cancel
Apply

> **NOTE**
> If this setting is enabled and the user's device is domain-joined, the associations configuration file is processed the next time the user signs on.

Set Microsoft Edge as the default browser on Azure Active Directory joined devices

To set Microsoft Edge as the default browser on Azure Active Directory joined devices follow the steps in the DefaultAssociationsConfiguration Mobile Device Management setting using the following application association file as an example.

```
<?xml version="1.0" encoding="UTF-8"?>
<DefaultAssociations>
  <Association ApplicationName="Microsoft Edge" ProgId="MSEdgeHTM" Identifier=".html"/>
  <Association ApplicationName="Microsoft Edge" ProgId="MSEdgeHTM" Identifier=".htm"/>
  <Association ApplicationName="Microsoft Edge" ProgId="MSEdgeHTM" Identifier="http"/>
  <Association ApplicationName="Microsoft Edge" ProgId="MSEdgeHTM" Identifier="https"/>
  <Association ApplicationName="Microsoft Edge" ProgId="MSEdgePDF" Identifier=".pdf"/>
</DefaultAssociations>
```

> **NOTE**
>
> To set Microsoft Edge Beta as the default browser, set **ApplicationName** to "Microsoft Edge Beta" and **ProgId** to "MSEdgeBHTML". To set Microsoft Edge Dev as the default browser, set **ApplicationName** to "Microsoft Edge Dev" and **ProgId** to "MSEdgeDHTML".

Set Microsoft Edge as the default browser on macOS

Attempting to programmatically set the default browser on macOS causes a prompt to appear for the end user. This prompt is a macOS security feature that can only be automated away by using an AppleScript.

Because of this limitation, there are two main methods for setting Microsoft Edge as the default browser on a macOS. The first option is to flash the device with an image of macOS where Microsoft Edge has already been set as the default browser. The other option is to use theSet Microsoft Edge as default browserpolicy, which prompts the user to set Microsoft Edge as the default browser.

When using either of these methods, it is still possible for a user to change the default browser. This is because for security reasons, the default browser preference can't be blocked programmatically. For this reason, we recommend that you deploy the **Set Microsoft Edge as default browser**policy even if you create an image with Microsoft Edge as the default browser. If the policy is set and a user changes the default browser from Microsoft Edge the next time they open Microsoft Edge, they will be prompted to set it as the default.

See also

- Plan your deployment of Microsoft Edge
- Microsoft Edge Enterprise landing page
- Set Microsoft Edge as default browser (Windows 7 and macOS)
- Windows 10 – How to configure file associations for IT Pros?
- Export or Import Default Application Associations
  - DISM Overview
  - DISM - Deployment Image Servicing and Management

Split tunnel VPN support for WebRTC (Web Real-Time Communication)

11/1/2022 • 2 minutes to read • Edit Online

This article describes Microsoft Edge and split tunnel VPN support for WebRTC. This support lets enterprise customers get the benefit of VPN split tunneling for peer-to-peer traffic on Microsoft Edge. VPN split tunneling improves peer-to-peer media streaming quality for users and reduces VPN server load.

> **NOTE**
> This article applies to Microsoft Edge version 96 or later.

What is VPN split tunneling and why should I use it?

VPN split tunneling is a feature that enables users to use two different networks for traffic instead of having all the traffic routed through a VPN. Windows has supported this feature for native applications, and VPN split tunneling is also offered for Microsoft 365 applications over VPN split tunneling on Windows. For more information, see Overview: VPN split tunneling with Office 365 - Microsoft 365 Enterprise. Microsoft Edge has also honored the VPN split tunneling configuration but support for the peer-to-peer traffic was missing.

We've heard about customers needs for routing peer-to-peer user traffic through their corporate network or cloud infrastructure over VPN.They werefrustrated about thequalityof video conference callsof their users on browsers compared tonative applications.As demonstrated by the native experience,VPN split-tunneling for peer-to-peer traffic can improve the quality of user video calls by routing it throughnormal Internetconnectionsinstead of VPN. It also can reduce the overall VPN server load by routing designated traffic off a VPN. Microsoft Edgenow brings this peer-to-peer traffic improvement toenterprise customers.

How to configure VPN split tunneling on Microsoft Edge

To enable VPN split tunneling and configure the networks for your users, we recommend you start with the guidance in Implementing VPN split tunneling for Office 365 - Microsoft 365 Enterprise. With the proper routing table configured based on the information described in the preceding article, you just need to take the additional step of enabling the WebRtcRespectOsRoutingTableEnabled policy. This policy enables support for Windows OS routing table rules when making peer to peer connections via WebRTC. Now you're ready to provide improved peer-to-peer media streaming experience on Microsoft Edge!

See also

- Microsoft Edge Enterprise landing page

What is Internet Explorer (IE) mode?

11/1/2022 • 3 minutes to read • Edit Online

NOTE

The retired, out-of-support Internet Explorer 11 (IE11) desktop application will be permanently disabled on certain versions of Windows 10 as part of the February 2023 Windows security update ("B") release scheduled for February 14, 2023. Learn more

We highly recommend setting up IE mode in Microsoft Edge and disabling IE11 prior to this date to ensure your organization does not experience business disruption. Learn how

We created Internet Explorer (IE) mode in Microsoft Edge for organizations that still need Internet Explorer 11 for backward compatibility with existing websites but also need a modern browser. This feature makes it easier for organizations to use one browser, for legacy web/apps or for a modern web/app. This article provides an introduction to using Microsoft Edge with IE mode.

For an advanced configuration guide, see Configure IE mode for Microsoft Edge.

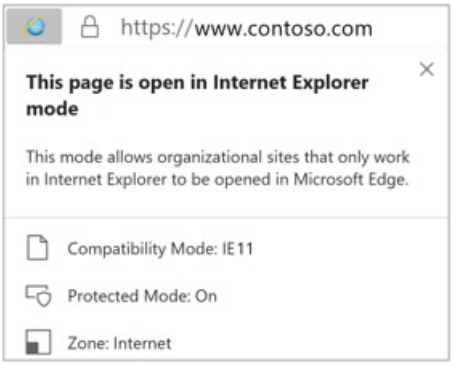
NOTE

This article applies to Microsoft Edge version 77 or later.

What is IE mode?

IE mode on Microsoft Edge makes it easy to use all of the sites your organization needs in a single browser. It uses the integrated Chromium engine for modern sites, and it uses the Trident MSHTML engine from Internet Explorer 11 (IE11) for legacy sites.

When a site loads in IE mode, the IE logo indicator displays on the left side of navigation bar. You can click the IE logo indicator to display additional information, as shown:


https://www.contoso.com
This page is open in Internet Explorer mode
This mode allows organizational sites that only work in Internet Explorer to be opened in Microsoft Edge.
Compatibility Mode: IE11
Protected Mode: On
Zone: Internet

Only those sites that you specifically configure (via policy) will use IE mode, all other sites will be rendered as modern web sites. For a site to use IE mode, you need to either:

- List the site in the Enterprise Mode Site List XML defined in one of these policies:
  - Microsoft Edge 78 or later, "Configure the Enterprise Mode Site List"

- Internet Explorer, "Use the Enterprise Mode IE website list"

> **NOTE**
> We only process one Enterprise Mode Site List. The Microsoft Edge site list policy takes precedence over the Internet Explorer site list policy.

- Configure the **Send all intranet sites to Internet Explorer** group policy and set it to **Enabled** (Microsoft Edge 77 or later.)

IE mode supports the following Internet Explorer functionality

- All document modes and enterprise modes
- ActiveX controls (such as Java or Silverlight). **Note**: Silverlight reaches end of support on October 12, 2021.
- Browser Helper Objects
- Internet Explorer settings and group policies that affect security zone settings and Protected Mode
- F12 developer tools for IE, when launched with IEChooser
- Microsoft Edge extensions (Extensions that interact with the IE page content directly are not supported.)

IE mode doesn't support the following Internet Explorer functionality

- Internet Explorer toolbars
- Internet Explorer settings and group policies that control the navigation menu.
- IE11 or Microsoft Edge F12 developer tools

Prerequisites

The following prerequisites apply to using Microsoft Edge with IE mode.

> **IMPORTANT**
> To ensure success, install the latest updates for Windows and Microsoft Edge. Failure to do so will likely cause IE mode to fail.

1. The minimum system updates for the operating systems listed in the next table.

OPERATING SYSTEM	VERSION	UPDATES
Windows 11		
Windows 10	1909 or later	
Windows 10	1903	KB4501375 or later
Windows Server	1903	KB4501375 or later
Windows 10	1809	KB4501371 or later
Windows Server	1809	KB4501371 or later
Windows Server	2019	KB4501371 or later
Windows 10	1803	KB4512509 or later

OPERATING SYSTEM	VERSION	UPDATES
Windows 10	1709	KB4512494 or later
Windows 10	1607	KB4516061 or later
Windows Server	2016	KB4516061 or later
Windows 10	initial version, July 2015	KB4520011 or later
Windows 8	8.1	KB4507463 or later; or KB4511872 or later
Windows Server	2012 R2	KB4507463 or later; or KB4511872 or later
Windows 8	Embedded	Install KB4492872 to upgrade to Internet Explorer 11; then install KB4507447 or later; or KB4511872 or later
Windows Server	2012	Install KB4492872 to upgrade to Internet Explorer 11; then install KB4507447 or later; or KB4511872 or later
Windows 7	SP1**	KB4507437 or later; or KB4511872 or later
Windows Server	2008 R2**	KB4507437 or later; or KB4511872 or later

IMPORTANT

** Windows 7 and Windows Server 2008 R2 will be supported by Microsoft Edge even after those operating systems go out of support. In order for IE mode to be supported on these operating systems the devices will need to have the Extended Security Updates for Windows 7. We recommend that you upgrade to a supported operating system as soon as possible in order to remain secure. Support for Microsoft Edge with the Extended Security Updates should be considered a temporary bridge to getting to a supported OS state.

2. The Microsoft Edge administrative template. For more information, see Configure Microsoft Edge.
3. Internet Explorer 11 enabled in Windows Features.

See also

- Microsoft Edge Enterprise landing page
- Additional Enterprise Mode information

Enterprise site configuration strategy

11/1/2022 • 2 minutes to read • Edit Online

NOTE

The retired, out-of-support Internet Explorer 11 (IE11) desktop application will be permanently disabled on certain versions of Windows 10 as part of the February 2023 Windows security update ("B") release scheduled for February 14, 2023. Learn more

We highly recommend setting up IE mode in Microsoft Edge and disabling IE11 prior to this date to ensure your organization does not experience business disruption. Learn how

This article describes changes to the Enterprise Mode Site List to support Internet Explorer mode for Microsoft Edge version 77 and later.

For more information on the schema for the Enterprise Mode Site List XML file, see Enterprise Mode schema v.2 guidance.

NOTE

This article applies to Microsoft Edge version 77 or later.

Configuration strategy

The following steps are part of a site configuration strategy for IE mode:

1. Prepare your site list
2. Configure neutral sites
3. (Optional) Use cookie sharing if necessary

Prepare your site list

If you already have an Enterprise Mode site list for IE11 or Microsoft Edge Legacy, you can reuse it to configure IE mode.

However, if you don't have a site list, you can use the Enterprise Site Discovery tool to populate your site list.

Configure neutral sites

In order for IE mode to work properly, authentication / Single Sign-On (SSO) servers will need to be explicitly configured as neutral sites. Otherwise, IE mode pages will try to redirect to Microsoft Edge, and authentication will fail.

A neutral site will use the browser where the navigation started - either Microsoft Edge or IE mode. Configuring neutral sites ensures that all applications using these authentication servers, both modern and legacy, continue to work.

You can configure neutral sites by setting the *Open In* dropdown to 'None' in the Enterprise Mode Site List Manager tool or by directly updating the site list XML:

```
<site url="login.contoso.com">

    <open-in>None</open-in>

</site>
```

To identify authentication servers, inspect the network traffic from an application using the IE11 Developer Tools. If you need more time to identify your authentication servers, you can configure a policy to keep all in-page navigations in IE mode to allow your users to continue their workflows uninterrupted. To minimize the use of IE mode when unnecessary, disable this setting once you've identified and added your authentication servers to the site list. For more information, see Keep in-page navigation in IE mode.

> **NOTE**
> Enterprise Mode schema v.1 isn't supported for IE mode integration. If you are currently using schema v.1 with Internet Explorer 11, you must upgrade to schema v.2. For more information, see Enterprise Mode schema v.2 guidance.

(Optional) Use cookie sharing if necessary

By default, the Microsoft Edge and Internet Explorer processes don't share session cookies, and this lack of sharing can be inconvenient in some cases while using IE mode. For example, when a user has to reauthenticate in IE mode when previously they are accustomed to doing so or when signing out of a Microsoft Edge session doesn’t sign out of the Internet Explorer mode session for critical transactions. In these scenarios, you can configure specific cookies set by SSO to be sent from Microsoft Edge to Internet Explorer so the authentication experience becomes more seamless by eliminating the need to reauthenticate. For more information, see Cookie sharing from Microsoft Edge to Internet Explorer.

See also

- Microsoft Edge Enterprise landing page
- About IE mode
- Additional Enterprise Mode information

Configure IE mode policies

11/1/2022 • 5 minutes to read • Edit Online

NOTE

The retired, out-of-support Internet Explorer 11 (IE11) desktop application will be permanently disabled on certain versions of Windows 10 as part of the February 2023 Windows security update ("B") release scheduled for February 14, 2023. Learn more

We highly recommend setting up IE mode in Microsoft Edge and disabling IE11 prior to this date to ensure your organization does not experience business disruption. Learn how

This article explains how to configure IE mode policies.

NOTE

This article applies to Microsoft Edge **Stable**, **Beta** and **Dev** Channels, version 77 or later.

Configuring IE mode requires three steps:

1. Configure Internet Explorer integration
2. Redirect sites from Microsoft Edge to IE mode
3. (Optional) Redirect sites from IE to Microsoft Edge
    a. If you are ready to disable the IE11 app, follow the steps in Disable Internet Explorer 11
    b. Otherwise, follow the rest of the steps in Redirect sites from IE to Microsoft Edge

NOTE

Policies to enable IE mode can be configured through Intune. For more information, see Add Microsoft Edge to Microsoft Intune and Configure Microsoft Edge policies with Microsoft Intune.

Configure Internet Explorer integration

You can configure Internet Explorer to open directly within Microsoft Edge (IE mode). You can also configure Internet Explorer to open with a standalone Internet Explorer 11 window. Most users prefer when sites open directly within Microsoft Edge in IE mode.

Enable Internet Explorer integration using Group Policy

1. Download and use the latest Microsoft Edge Policy Template.
2. Open Group Policy Editor.
3. Click **User Configuration/Computer Configuration** > **Administrative Templates** > **Microsoft Edge**.
4. Double-click **Configure Internet Explorer integration**.
5. Select **Enabled**.

6. Under **Options**, set the dropdown value to

   - **Internet Explorer mode** if you want sites to open in IE mode on Microsoft Edge
   - **Internet Explorer 11** if you want sites to open in a standalone Internet Explorer 11 window (This option will not be supported after June 15, 2022 when the Internet Explorer 11 desktop application will be retired and go out of support. After June 15, 2022 when IE11 will no longer be available, this option will behave the same as the **Internet Explorer mode** option.)
   - **None** if you want to stop users from configuring Internet Explorer mode via edge://flags or through the command line

   > **NOTE**
   > Setting the policy to **Disabled** implies IE mode is disabled by policy, but can be set through edge://flags or command line options.

7. Click **OK** or **Apply** to save this policy setting.

Redirect sites from Microsoft Edge to IE mode

There are two options for identifying which sites should open in IE mode:

- (Recommended) Configure sites on the Enterprise Site list
- Configure all Intranet sites

Configure sites on the Enterprise Site list

You can use the following group policies to configure specific sites to open in IE mode:

- Use the Enterprise Mode IE website list (Internet Explorer)
- Configure the Enterprise Mode Site List (Microsoft Edge, version 78 or later)
  This policy lets you create a separate Enterprise Mode Site list for Microsoft Edge. Enabling this policy overrides the settings in the "Use the Enterprise Mode IE website list" policy, if "Configure Internet Explorer integration" is enabled. Disabling or not configuring this policy doesn't affect the default behavior of the "Configure Internet Explorer integration" policy.

  > **NOTE**
  > It is not mandatory to configure the Microsoft Edge policy. Many organizations use this as an override, allowing them to target the current Site List at all users with the IE policy, and more easily target an updated version to pilot uses with the Microsoft Edge policy.

For more information about Enterprise Mode Site Lists, see Use the Enterprise Site List Manager.

Configure using the Use the Enterprise Mode IE website list policy

IE mode can use the existing policy configuring the Enterprise Site List for Internet Explorer, allowing you to create and maintain a single list.

1. Create or reuse a Site List XML
   a. All sites that have the element *<open-in>IE11</open-in>* will now open in IE mode.
2. Open Group Policy Editor.
3. Click **User Configuration/Computer Configuration** > **Administrative Templates** > **Windows Components** > **Internet Explorer**.
4. Double-click **Use the Enterprise Mode IE website list**.
5. Select **Enabled**.
6. Under **Options**, type the location of website list. You can use one of the following locations:

- (Recommended) HTTPS location: **https://iemode/sites.xml**
- Local network file:**\\network\shares\sites.xml**
- Local file: **file:///c:/Users/<user>/Documents/sites.xml**

7. Click **OK** or **Apply** to save these settings.

Configure using the Configure the Enterprise Mode Site List policy

You can also configure IE mode with a separate policy for Microsoft Edge. This additional policy allows you to override the IE site list. For example, some organizations will target the production site list to all users. You can then deploy the pilot site list to a small group of users using this policy.

1. Create or reuse a Site List XML
   a. All sites that have the element *<open-in>IE11</open-in>* will now open in IE mode.
2. Open Group Policy Editor.
3. Click **User Configuration/Computer Configuration** > **Administrative Templates** > **Microsoft Edge**.
4. Double-click **Configure the Enterprise Mode Site List**.
5. Select **Enabled**.
6. Under **Options**, type the location of website list. You can use one of the following locations:
   - (Recommended) HTTPS location: **https://iemode/sites.xml**
   - Local network file: **\\network\shares\sites.xml**
   - Local file: **file:///c:/Users/<user>/Documents/sites.xml**
7. Click **OK** or **Apply** to save these settings.

Configure all intranet sites

IE mode can be configured as for all sites in the Local Intranet zone. You can remove individual sites from IE mode using an Enterprise Mode Site List.

> **NOTE**
> The Local Intranet zone contains explicitly added sites, but also assigns sites to this zone using heuristics. This can include dotless host names (e.g. **https://payroll**) and sites that the proxy configuration script configures to bypass the proxy. If an external party controls DNS or proxy, they could potentially force websites into IE mode.

1. Open Local Group Policy Editor.
2. Click **User Configuration/Computer Configuration** > **Administrative Templates** > **Microsoft Edge**.
3. Double-click **Send all intranet sites to Internet Explorer**.
4. Select **Enabled**, and then click **OK** or **Apply** to save the policy settings.

Redirect sites from IE to Microsoft Edge

You can prevent your users from using Internet Explorer for sites that don't need it. Internet Explorer can automatically redirect sites to Microsoft Edge if they aren't on your site list.

1. Open Group Policy Editor.
2. Click **User Configuration/Computer Configuration** > **Administrative Tools** > **Windows Components** > **Internet Explorer**.
3. Double-click **Send all sites not included in the Enterprise Mode Site List to Microsoft Edge.**
4. Select **Enabled**
5. Click **OK** or **Apply** to save these settings.
6. Double-click **Configure which channel of Microsoft Edge to use for opening redirected sites**.

7. Select **Enabled**.
8. Under **Options**, select your top three choices for the channel to use - Internet Explorer will redirect to the highest ranked choice that the user has installed on that device:
    - Microsoft Edge Stable
    - Microsoft Edge Beta version 77 or later
    - Microsoft Edge Dev version 77 or later
    - Microsoft Edge Canary version 77 or later
    - Microsoft Edge version 45 or earlier
9. Click **OK** or **Apply** to save these settings.

> **TIP**
> To find sites that you need to add to your IE mode site list, see Configure IE mode for Microsoft Edge guide. If you already have a site list, the tools in this guide will help you apply it to the right users.

See also

- Microsoft Edge Enterprise landing page
- About IE mode
- Additional Enterprise Mode information

Cloud Site List Management for Internet Explorer (IE) mode

11/1/2022 • 18 minutes to read • Edit Online

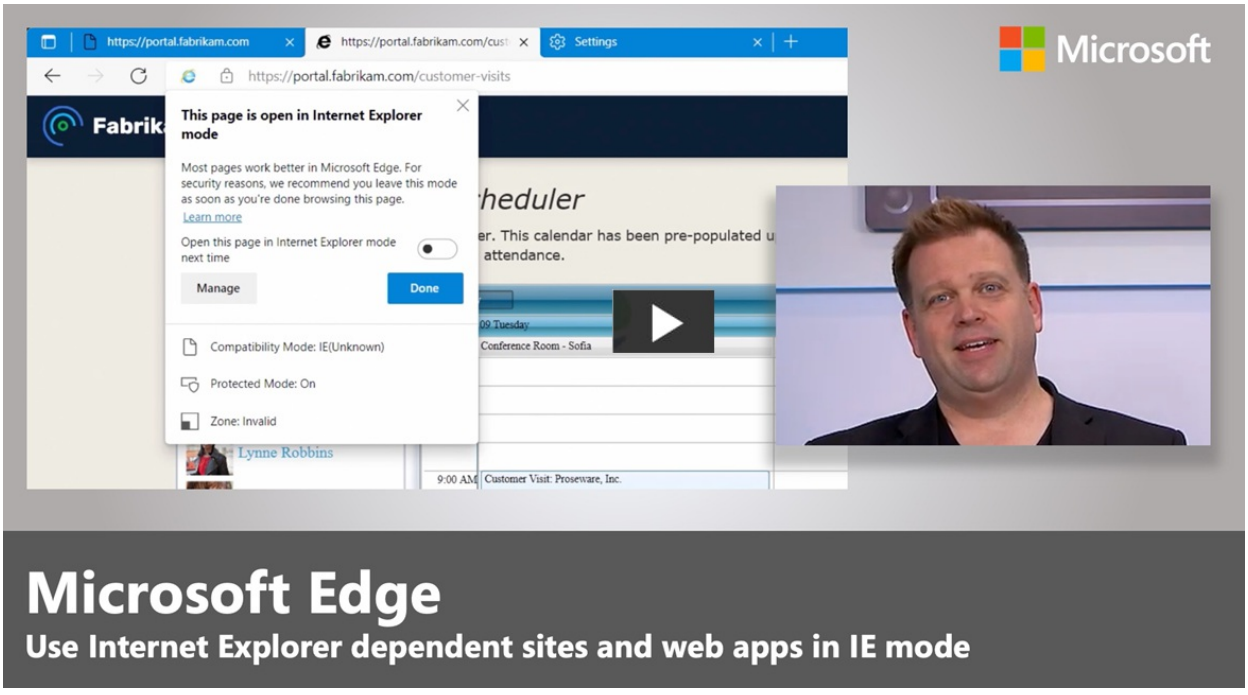
This article explains how to configure and use Cloud Site List Management for Internet Explorer (IE) mode through the Microsoft 365 Admin Center.

> **NOTE**
> This user experience is currently only available to worldwide and GCC cloud instances.

Overview

As you transition your workflows and applications from IE11 to IE mode, **Cloud Site List Management** lets you manage your site lists for IE mode in the cloud. You can work with site lists using the **Microsoft Edge Site Lists** experience in the **Microsoft 365 Admin Center**.

To learn more, watch the next video.


Microsoft
This page is open in Internet Explorer mode
Most pages work better in Microsoft Edge. For security reasons, we recommend you leave this mode as soon as you're done browsing this page.
Learn more
Open this page in Internet Explorer mode next time
Manage
Done
Compatibility Mode: IE(Unknown)
Protected Mode: On
Zone: Invalid
Microsoft Edge
Use Internet Explorer dependent sites and web apps in IE mode

This experience lets you store your organization's site list in a compliant cloud location instead of needing an on-premises infrastructure to host your site list. You can create, import, export site lists, and audit changes to site list entries through the Microsoft 365 Admin Center. You can publish multiple site lists to the cloud and use group policy to assign different groups of devices to use different lists.

Prerequisites

The following prerequisites apply to this feature.

1. Customers must have an Azure AD tenant.
2. Admins must have Microsoft Edge version 93 or greater installed and the latest version of the policy files.
3. Admins need to be an Microsoft Edge Administrator or a Global Administrator on the tenant to access the

Microsoft Edge site lists experience.

Cloud Site List Management experience

There are four aspects to the Cloud Site List Management experience:

- Publishing the enterprise site list to the cloud.
- Associating the cloud site list with Microsoft Edge.
- Managing site list contents on the Microsoft 365 Admin Center.
- Viewing site feedback on the Microsoft 365 Admin Center.

Publish enterprise site list to the cloud

Admins can publish one or more site lists to an authenticated endpoint that Microsoft Edge clients within their tenant can download for the IE mode experience. Admins can import the existing enterprise site list XML into the Microsoft Edge Site Lists experience in the Microsoft 365 Admin Center and then publish it to the cloud location.

Associate the cloud-hosted site list with Microsoft Edge

With Microsoft Edge version 93, admins can use the InternetExplorerIntegrationCloudSiteList setting to configure one of the cloud-hosted site lists that Microsoft Edge can consume for IE mode. Users must be signed in to Microsoft Edge for the client to consume the site list from the cloud.

> **IMPORTANT**
> When this policy is configured, it overrides the original InternetExplorerIntegrationSiteList policy.

Manage site list contents on the Microsoft 365 Admin Center

Admins can create a new list or import an existing site list into the Microsoft Edge site lists experience. They can add, edit, delete site list contents, and view comment history to track changes to individual entries. The next section explains how to opt in to public preview and access the Microsoft Edge site lists experience in the Microsoft 365 Admin Center.

Manage site feedback on the Microsoft 365 Admin Center

With Microsoft Edge version 99, admins can use the InternetExplorerIntegrationCloudUserSitesReporting and InternetExplorerIntegrationCloudNeutralSitesReporting policies to identify gaps in their site list with site feedback. They can view sites that users have added to their local site lists, and potentially misconfigured neutral sites.

Publish enterprise site list to the cloud

Use the following steps as a guide to create a site list, import a site list, and publish a site list. Before you can complete these steps, sign in the Microsoft 365 admin center.

1. Sign in to the Microsoft 365 admin center with your admin credentials.
2. On the left navigation pane, select **Settings > Org settings**.
3. You'll see the **Microsoft Edge site lists** option.

> **NOTE**
> If you don't see this option on the Org settings page while we are rolling out to all production instances, you'll need to opt in to **Targeted release**. If you don't see the **Microsoft Edge site lists** option, see this FAQ: I don't see the "Microsoft Edge site lists" option in the "Org settings" page on Microsoft 365 Admin Center. Why is that?.

Steps to create a site list

1. On the Org settings page, select **Microsoft Edge site lists**
2. On the resulting page, select **Create a new list**.
3. Enter a **Site list name** and a **Description**, and then select **Create**.
4. After you get confirmation, select **Close panel**.

Steps to import a site list

1. Select the site list you want to populate.
2. On the resulting page, select **Import list**.
3. On the right-hand panel, select **Browse**.
4. Select the file you want to import and then select **Upload** on the bottom of the panel.
5. You can skim through the URLs in the uploaded file. If you want to pick a different file, you can select **Upload a different file** at the top of the panel. If everything looks correct, select **Add** at the bottom of the panel.
6. After your list is imported, select **Close panel**.

Steps to publish a site list

1. To publish a site list, go back up a level to the Microsoft Edge site lists page. Select the breadcrumb above the site list name to go up a level.
2. On the Microsoft Edge site lists page, select the site list you want to publish to the cloud, and then select **Publish site list**.
3. On the right-hand panel, update the **Version number** and select **Publish** the bottom of the panel.
4. After confirmation, select **Close panel**.
5. The **Published status** column, **Last published**, and **Last published by** are all updated.

Associate the cloud-hosted site list with Microsoft Edge

Use the following steps to associate the cloud-hosted site list with Microsoft Edge.

1. To configure devices to use a published site list, select the site list you want to assign to devices.
2. On the resulting page, copy the **Site list ID**.
3. For the device group you pick, select **Enabled** and enter the **Site list ID** in the Configure the Enterprise Mode Cloud Site List policy.
4. You can run **gpupdate/force** from the Command Prompt to update the device with the policy or wait for the group policy to take effect. After the policy is updated, you can verify that Microsoft Edge is reading the cloud site list by going to edge://compat/enterprise. You need to be signed into Microsoft Edge.

> **NOTE**
>
> After publishing a site list the first time and updating group policy, you need to restart Microsoft Edge. Wait 60 seconds or select the **Force Update** button on edge://compat/enterprise. When publishing updates to an already associated site list, there may be an older version of the site list in the cache. This entry will be refreshed after 60 seconds. For more information, see What happens if users log out of Microsoft Edge?.

Manage site list contents on the Microsoft 365 Admin Center

You can add, edit, delete site list contents, and view comment history to track changes to individual entries for sites and shared session cookies.

> **NOTE**
> Persistent-cookies, which have been created with an `Expires-attribute`, can't be shared between Microsoft Edge and Internet Explorer.

If you have hybrid scenarios that require your site list to be hosted on-premises, you can export your site list from the Microsoft 365 Admin Center. Use the following steps as a guide for managing site list content.

Add a site to the site list

You can add individual sites to any site list. After adding sites to the list, you can use the predefined filters using the **Filter** button (next to the Search box) to view updates to the list.

1. Go to the site list where you want to add a site.
2. Select **Add a site**.
3. Enter the site address and pick the engine that should be used to open the site. Add comments as needed and then select **Save**.

   > **NOTE**
   > The **Status** column for any entries added to a published site list will show **Addition pending**. If you navigate to the list of site lists by selecting **Microsoft Edge site lists** at the top of the screen, you'll see that the **Published Status** column shows **Changes pending publish** to indicate that latest updates to the site list need to be published in order for users to receive them. You can use the **Filter** button (next to the Search box) to select **Addition pending** to see all the added entries that are pending publication.

Delete a site from the site list

Use the following steps to delete a site entry.

1. Pick the site entry that you'd like to delete from the site list. Select **Delete site**.
2. Select **Delete** in the dialog pop-up.
3. After you see confirmation that a site entry has been deleted, it will stay on the list until the site list is published to the cloud location. You can view the list of deleted sites before publishing by selecting the **Filter** button and filtering for sites in the **Delete pending** state.

   > **NOTE**
   > The **Status** column for any entries deleted from a published site list will show **Delete pending**. If you navigate to the list of site lists by selecting **Microsoft Edge site lists** at the top of the screen, you'll see that the **Published Status** column shows **Changes pending publish** to indicate that latest updates to the site list need to be published in order for users to receive them. You can use the **Filter** button (next to the Search box) to select **Delete pending** to see all deleted entries that are pending publication.

View the change history for site entries

To view the change history for site entries:

- Select the site entry that you want to see the change history for, and then select **View history**.

Copy a site to other site lists

Use the following steps to copy a site entry from a site list to one or more site lists.

1. Pick a site entry that you'd like to copy to another list. Select **Copy to more lists**.

2. Select one or more site lists you'd like to copy to from the dropdown list.
3. Select **Copy site** at the bottom of the panel.
4. After you see confirmation that a site entry has been copied, it will stay on the site list you copied it from. It will also appear on the site list(s) you copied it to.

> **NOTE**
>
> The **Status** column for any entries copied to a published site list will show **Addition pending**. If you navigate to the list of site lists by selecting **Microsoft Edge site lists** at the top of the screen, you'll see that the **Published Status** column shows **Changes pending publish** to indicate that latest updates to the site list need to be published in order for users to receive them. You can use the **Filter** button (next to the Search box) to select **Addition pending** to see all the added entries that are pending publication.

Add a shared session cookie to the site list

You can add individual shared session cookies to any site list. After adding shared cookies to the list, you can use the predefined filters using the **Filter** button (next to the Search box) to view updates to the list.

1. Go to the site list where you want to add a shared cookie.
2. Select **Add a shared cookie**.
3. Enter the domain and cookie name. Add comments as needed and then select **Save**.

> **NOTE**
>
> The **Status** column for any entries added to a published site list will show **Addition pending**. If you navigate to the list of site lists by selecting **Microsoft Edge site lists** at the top of the screen, you'll see that the **Published Status** column shows **Changes pending publish** to indicate that latest updates to the site list need to be published for users to receive them. You can use the **Filter** button (next to the Search box) to select **Addition pending** to see all the added entries that are pending publication.

Delete a shared session cookie from the site list

Use the following steps to delete a shared session cookie entry.

1. Pick the entry that you'd like to delete from the site list. Select **Delete shared cookie**.
2. Select **Delete** in the dialog pop-up.
3. After you see confirmation that an entry has been deleted, it will stay on the list until the site list is published to the cloud location. You can view the list of deleted shared cookies before publishing by selecting the **Filter** button and filtering for cookies in the **Delete pending** state.

> **NOTE**
>
> The **Status** column for any entries deleted from a published site list will show **Delete pending**. If you navigate to the list of site lists by selecting **Microsoft Edge site lists** at the top of the screen, you'll see that the **Published Status** column shows **Changes pending publish** to indicate that latest updates to the site list need to be published for users to receive them. You can use the **Filter** button (next to the Search box) to select **Delete pending** to see all deleted entries that are pending publication.

View the change history for shared session cookies

To view the change history for shared session cookies:

- Select the entry that you want to see the change history for, and then select **View history**.

Copy a shared session cookie to other site lists

Use the following steps to copy a shared session cookie entry from a site list to one or more site lists.

1. Pick an entry that you'd like to copy to another list. Select **Copy to more lists**.
2. Select one or more site lists you'd like to copy to from the dropdown list.
3. Select **Copy cookie** at the bottom of the panel.
4. After you see confirmation that a site entry has been copied, it will stay on the site list you copied it from. It will also appear on the site list(s) you copied it to.

> **NOTE**
>
> The **Status** column for any entries copied to a published site list will show **Addition pending**. If you navigate to the list of site lists by selecting **Microsoft Edge site lists** at the top of the screen, you'll see that the **Published Status** column shows **Changes pending publish** to indicate that latest updates to the site list need to be published in order for users to receive them. You can use the **Filter** button (next to the Search box) to select **Addition pending** to see all the added entries that are pending publication.

Export a site list

There are scenarios where you want to export a site list. For example, if you're unable to move your site list to the cloud right away or if you need to maintain a hybrid environment with site lists in the cloud and on-premises. You can use the Cloud Site List Management experience to manage updates to a site list in a central location and export the site list to the on-premises host.

To export a site list:

1. On the Microsoft Edge site lists page, select the site list that you want to export.
2. Select **Export list** to download the site list XML file

Restore a previous version of a site list

Use the following steps as a guide to restore the previous version of a site list.

> **NOTE**
>
> Only the last 3 published versions of a site list are saved. When you publish more than 3 versions, the saved version with the lowest version number will be permanently deleted, and you will no longer be able to restore that version. If you want to keep a copy of a site list, you should export it before publishing a new version.

1. On the Microsoft Edge site lists page, select the list that you'd like to restore to a previous version.
2. Select a previous version from the **Version** dropdown list.
3. You can view the contents of a previous version of the site list. You can also export it if you want to save a copy by selecting **Export** in the message bar.
4. After picking the version you want to restore, select **Restore** in the message bar.
5. If you have unpublished changes in the current version of the site list, you can choose to include them by selecting the checkbox in the panel.

   > **NOTE**
   >
   > If you don't include the unpublished changes, they will be lost when you restore the previous version.

6. Select **Restore** at the bottom of the panel to restore the previous version.

Manage site feedback on the Microsoft 365 Admin Center

The Site feedback tab shows the sites that users are adding to their local IE Mode site list, and potentially misconfigured neutral sites reported by Microsoft Edge. You'll see the site address, the number of users who are adding this site, and which published, cloud-hosted site lists the feedback came from. You can act on an individual entry by adding it to an existing site list(s), pausing, or deleting the feedback. You can also view change history and comments.

Add a site to site lists

Use the following steps to add a site to one or more site lists from site feedback.

1. Pick the entry that you want to add. Select **Add to site lists**.
2. Select one or more site lists to add to from the dropdown. Pick the engine that should be used to open the site and add comments as needed.
3. Select **Add site** at the bottom of the panel.

> **NOTE**
> The status for this entry will update to **Resolved** because it was **Added**. This site will now appear on the site list(s) you selected.

Pause incoming feedback on a site

You can postpone acting on a pending entry by pausing feedback. You can pause feedback for 30 days or indefinitely. Use the following steps to pause incoming feedback.

1. Pick an entry that you want to pause feedback on. Select **Pause Feedback**.
2. Add comments as needed and select how long you'd like to pause feedback for.
3. Select **Pause** at the bottom of the panel.

> **NOTE**
> The status for this entry will update to **Resolved** because it was **Paused**. If you paused for 30 days, then after 30 days if there's any incoming feedback, the entry's status will refresh back to **Pending** for you to act on.

Delete feedback on a site

Use the following steps to delete a feedback entry.

1. Pick the entry that you want to delete. Select **Delete feedback**.
2. Select **Delete** on the pop-up dialog.

> **NOTE**
> If you delete an entry, it might reappear in the future as incoming feedback if users continue to add the site to their local site lists or if Microsoft Edge detects it as a potentially misconfigured neutral site.

View the change history for site feedback entries

To view the change history:

- Select the entry that you want to see the change history for, and then select **Feedback history** in the side panel.

FAQ

I don't see the "Microsoft Edge site lists" option in the "Org settings" page on Microsoft 365 Admin Center. Why is that?

The experience will be available when rollout completes by mid-December. While the experience is rolling out, you'll need to opt in to view this experience in the Microsoft 365 Admin Center. You must be a global admin in Microsoft 365 to opt in.

You can use the following steps to opt in:

1. Sign in to the Microsoft 365 Admin Center and then go to **Settings** > **Org settings**. Under the **Organization profile** tab, choose **Release preferences**.
2. To disable targeted release, select **Standard release**, then select **Save changes**.
3. To enable targeted release for all users in your organization, select **Targeted release for everyone**, then select **Save changes**.
4. To enable targeted release for some people in your organization, select **Targeted release for selected users**, then select **Save changes**.
5. Choose **Select users** to add users one at a time, or **Upload users** to add them in bulk.
6. When you finish adding users, select **Save changes**.

For more information, see Set up the Standard or Targeted release options - Microsoft 365 admin

When I select "Microsoft Edge site lists" and try to create a new list, I get this error - "Request failed with status code 500". Why is that?

Microsoft Edge Site Lists stores its data and configuration in a service infrastructure that's shared with enterprise cloud services such as Exchange Online, SharePoint Online, Teams, and Azure Active Directory. In rare cases, when Microsoft Edge site lists is the first feature to use this infrastructure, provisioning might take some time. In these cases, the initial request from the Microsoft 365 Admin Center will fail. When the request fails, an alert is sent to the provisioning system to address the problem. Typically provisioning completes in three days. Therefore, if you get this error, try again in a few days and create a new list. If you still can't create a new list, or if you need urgent assistance, contact Microsoft Support.

Can users who haven't signed in to Microsoft Edge download the site list?

No, users must sign in to the browser to download the cloud hosted site list. You can configure a policy to allow Implicit Sign in to prevent user experience disruption. For more information, see ImplicitSignInEnabled.

What is the default refresh interval after updates are made to site list contents?

The site list is refreshed in Microsoft Edge every two hours. You can change this interval in the InternetExplorerIntegrationSiteListRefreshInterval policy. The minimum refresh interval is 30 minutes.

What happens if users log out of Microsoft Edge?

Access to the site list requires explicit browser sign in for the first download. In a scenario where the user logs out after being logged in, the site list is cached in Microsoft Edge. The list will stay cached even if the user logs out of Microsoft Edge from their Azure Active Directory (Azure AD) account. Microsoft Edge won't try to fall back to the non-cloud download location while the Cloud site list policy is configured. Microsoft Edge attempts to update the cached site list at the following times (note that all attempts will fail if the user isn't signed in to Microsoft Edge):

- 60 seconds after you restart the browser.
- Every two hours when Microsoft Edge is running. The 120-minute refresh interval can be changed by using the InternetExplorerIntegrationSiteListRefreshInterval policy. The minimum refresh interval is 30 minutes.

Where is the cloud site list hosted?

The data is stored in Substrate Data Store which ensures that the data is stored in a compliant location and

confers to local data handling rules. Substrate decides what region the data is stored based on the geo location you have chosen for your tenant.

Support and Feedback

Support for Cloud Site List Management experience is covered by your existing Microsoft Premier Support contract. You can reach out to Microsoft Support to report issues or feedback. You can also leave feedback in our TechCommunity forum.

See also

- About IE mode
- Microsoft Edge Enterprise landing page

Configure local site list for Internet Explorer (IE) mode

11/1/2022 • 5 minutes to read • Edit Online

> **NOTE**
> The retired, out-of-support Internet Explorer 11 (IE11) desktop application will be permanently disabled on certain versions of Windows 10 as part of the February 2023 Windows security update ("B") release scheduled for February 14, 2023. Learn more
>
> We highly recommend setting up IE mode in Microsoft Edge and disabling IE11 prior to this date to ensure your organization does not experience business disruption. Learn how

This article explains how to configure easy access to Internet Explorer mode (IE mode) and allow the use of local site lists in your organization.

> **NOTE**
> This article applies to Microsoft Edge version 92 or later.

Prerequisites

1. Windows updates
   - Windows 11
   - Windows 10, version 1809; Windows Server 2019 - KB5015880 or later
   - Windows 10, version 1909 - KB5003974 and KB5003698 or later
   - Windows 10, version 2004; Windows 10, version 20H2 and Windows 10, version 21H - KB5005260 and KB5005101 or later
2. Microsoft Edge version 92 (92.0.902.55 or later)

> **IMPORTANT**
> This local site list feature isn't supported on Windows Server 2016 at this time.

Overview

IE mode is powered by the configuration of the Enterprise Mode Site List. While you're identifying and configuring sites on the site list to use IE mode, your users no longer need to wait or fall back to the standalone IE11 application.

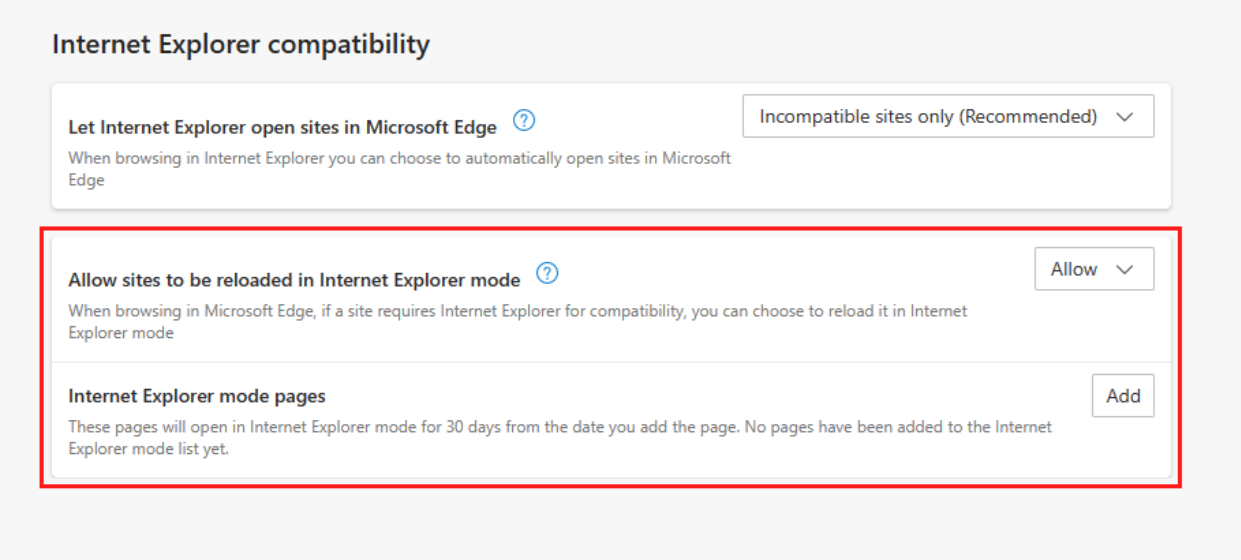
Starting with Microsoft Edge version 92, repeated access to *unconfigured* IE mode sites is easier. Users can reload sites in IE mode. They can add these sites to their local site list to automatically render in IE mode for 30 days, while the organization's site list gets updated. When IE11 is disabled in your environment, your users are no longer solely dependent on the organization's site list.

You can configure this experience through group policies for your organization.

> **NOTE**
>
> An *unconfigured* site is one that requires IE mode but isn't configured to open in IE mode in the Enterprise Mode Site List.

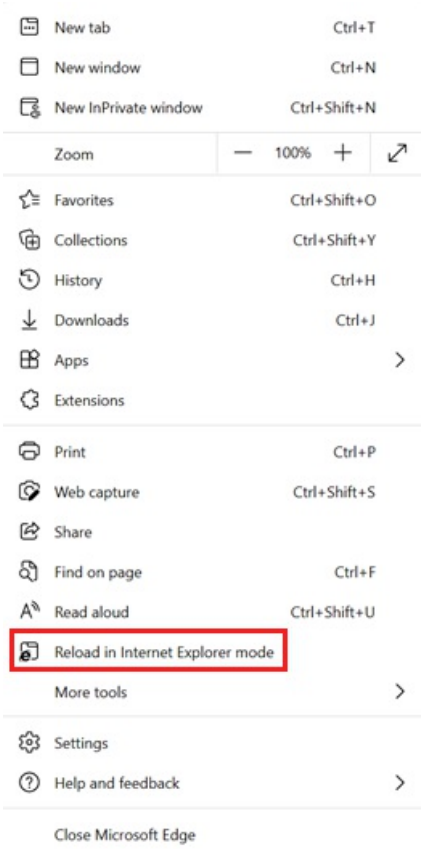
Enable the local site list experience

To enable the local site list experience, users can go to the URL *edge://settings/defaultBrowser* and set **Allow sites to be reloaded in Internet Explorer mode** to **Allow**.


Internet Explorer compatibility
Let Internet Explorer open sites in Microsoft Edge
When browsing in Internet Explorer you can choose to automatically open sites in Microsoft Edge
Incompatible sites only (Recommended)
Allow sites to be reloaded in Internet Explorer mode
When browsing in Microsoft Edge, if a site requires Internet Explorer for compatibility, you can choose to reload it in Internet Explorer mode
Allow
Internet Explorer mode pages
These pages will open in Internet Explorer mode for 30 days from the date you add the page. No pages have been added to the Internet Explorer mode list yet.
Add

> **NOTE**
>
> 1. If you have enabled IE mode testing through the *InternetExplorerIntegrationTestingAllowed* policy, you will see this setting, but it will be greyed out unless you explicitly enable the *InternetExplorerIntegrationReloadInIEModeAllowed* policy.
> 2. If **Allow sites to be reloaded in Internet Explorer mode** is set to **Default**, users might be able to reload sites in IE mode if they have existing Internet Explorer 11 usage.

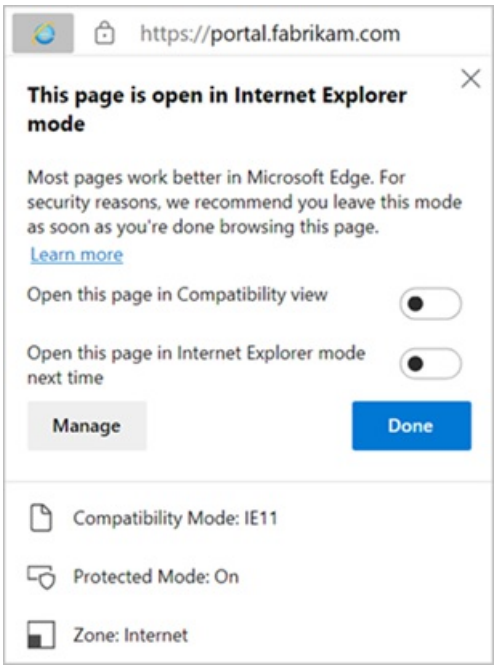
When this setting is enabled, users can reload a site in IE mode by selecting **Settings and more (the ellipses icon ...) > Reload in Internet Explorer mode**. Users can also select **Reload tab in Internet Explorer mode** when they right-click on a tab or choose **Open link in new Internet Explorer mode tab** when they right-click on a link.



The **Reload in Internet Explorer mode** icon can be pinned to the toolbar. The toolbar button allows users to easily enter and exit IE mode and can be managed through the *edge://settings/appearance* URL.

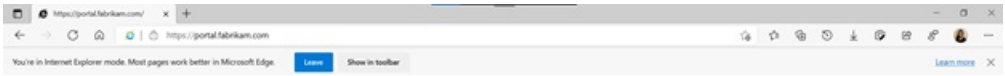
> **NOTE**
>
> If the user is on a site that's already in the organization's Enterprise Mode Site List, options to Reload in (or Exit) Internet Explorer mode will be visible but greyed out.

When the option is selected, the site reloads in IE mode. The IE mode indicator icon is visible to the left of the address bar. The flyout shows an option that users can toggle to **Open the page in Compatibility view** which adds the page to the Internet Explorer Compatibility view settings list and refreshes the page. Also, there's an option that users can toggle to **Open the page in Internet Explorer mode** next time. This adds the specific page the user is on to the local site list and will automatically open in IE mode for the next 30 days.


https://portal.fabrikam.com
This page is open in Internet Explorer mode
Most pages work better in Microsoft Edge. For security reasons, we recommend you leave this mode as soon as you're done browsing this page.
Learn more
Open this page in Compatibility view
Open this page in Internet Explorer mode next time
Manage
Done
Compatibility Mode: IE11
Protected Mode: On
Zone: Internet

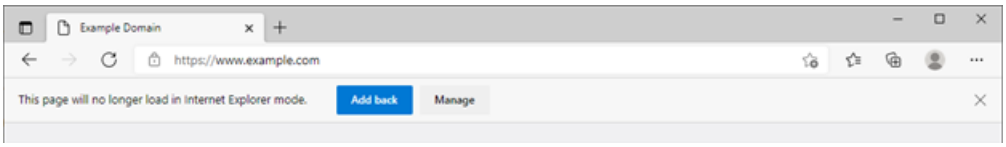
After a site has been reloaded in IE mode, "in-page" navigation will stay in IE mode (for example, a link, script, a form on the page, or a server-side redirect from another "in-page" navigation).

While in IE mode, users will see a banner indicating they are in IE mode, the option to Leave IE mode,, and to pin the IE mode icon to the toolbar (if it isn't pinned already).



Users can choose to exit from IE mode using the Leave button on the banner, the pinned IE mode icon or **Settings and more (the ellipses icon ...) > Exit Internet Explorer mode**, otherwise Microsoft Edge will automatically exit from IE mode when a navigation that isn't "in-page" occurs (for example, using the address bar, the back button, or a favorite link).

Entries remain on the local site list for a default period of 30 days. We recommend you configure legacy sites for your organization in the Enterprise Mode Site List. The local site list will ensure that users can continue their workflow without being interrupted while the organization's site list gets updated. On day 31, when users navigate to the site, they'll see a banner explaining that the site will no longer load in IE mode. Users can add it back to the local site list if they so choose.



Policies to configure the use of local site lists for IE mode

Two group policies are available to configure the local site list experience in Microsoft Edge. These policies are:

Policy: InternetExplorerIntegrationReloadInIEModeAllowed

This policy corresponds to the Microsoft Edge setting "Allow sites to be reloaded in Internet Explorer mode". You can access this setting by going to the *edge://settings/defaultbrowser* URL.

- If you enable this policy, users can reload a site in IE mode by selecting **Settings and more (the ellipses icon ... > Reload in Internet Explorer mode**. Users can also select **Reload tab in Internet Explorer mode** when they right-click on a tab, or choose **Open link in new Internet Explorer mode tab** when they right click on a link. Users can optionally tell Microsoft Edge to use IE mode for the site in the future. This choice will be remembered for a default of 30 days and can be managed using the policy

InternetExplorerIntegrationLocalSiteListExpirationDays.

- If you disable this policy, users won't be allowed to reload an unconfigured site in IE mode.
- If you don’t configure this policy, we'll show users options to reload unconfigured sites in IE mode depending on recent Internet Explorer 11 usage.

Note that this policy takes precedence over how you configured the InternetExplorerIntegrationTestingAllowed policy and that policy will be disabled.

Policy: InternetExplorerIntegrationLocalSiteListExpirationDays

This policy can be used to adjust the number of days that a site remains on the local site list for users.

- If you disable or don’t configure this policy, a default value of 30 days is used.
- If you enable the policy, you must enter a value between 0-90 days to keep the site on a user’s local site list.

This policy has no effect if you disabled the *InternetExplorerIntegrationReloadInIEModeAllowed* policy.

> **NOTE**
> The local site list currently doesn't sync across devices. This improvement is currently in our backlog and we’ll update this feature when it's available.

See Also

- Disable Internet Explorer 11 - Disable Internet Explorer 11
- Configure IE mode policies - Configure IE mode Policies

Disable Internet Explorer 11

11/1/2022 • 3 minutes to read • Edit Online

NOTE

The retired, out-of-support Internet Explorer 11 (IE11) desktop application will be permanently disabled on certain versions of Windows 10 as part of the February 2023 Windows security update ("B") release scheduled for February 14, 2023. Learn more

We highly recommend setting up IE mode in Microsoft Edge and disabling IE11 prior to this date to ensure your organization does not experience business disruption. Learn how

This article describes how to disable Internet Explorer 11 as a standalone browser in your environment.

Prerequisites

The following Windows updates and Microsoft Edge software are required:

- Windows updates
  - Windows 10, version 21H1 or later
  - Windows 10, version 2004; Windows Server version 2004; Windows 10, version 20H2; Windows Server version 20H2: KB4598291 or later
  - Windows 10 version 1909: KB4598298 or later
  - Windows Server 2019; Windows 10 Enterprise 2019 LTSC: KB4598296 or later
  - Windows Server 2016; Windows 10 Enterprise 2016 LTSB: KB4601318 or later
  - Windows 10 Enterprise 2015 LTSB: KB4601331 or later
  - Windows 8.1; Windows Server 2012 R2: KB4601384 or later
  - Windows Server 2012: KB4601348 or later
- Microsoft Edge Stable Channel

Overview

For organizations that require Internet Explorer 11 (IE11) for legacy compatibility, Internet Explorer mode (IE mode) on Microsoft Edge provides a seamless, single browser experience. Users can access legacy applications from within Microsoft Edge without having to switch back to IE11.

After you configure IE mode, you can disable IE11 as a standalone browser **without affecting IE mode functionality** across your organization using group policy.

NOTE

If you need the standalone IE11 app for specific sites, and want to redirect all other browser traffic to Microsoft Edge, you can configure the Send all sites not included in the site list to Microsoft Edge policy to redirect sites from IE to Microsoft Edge.

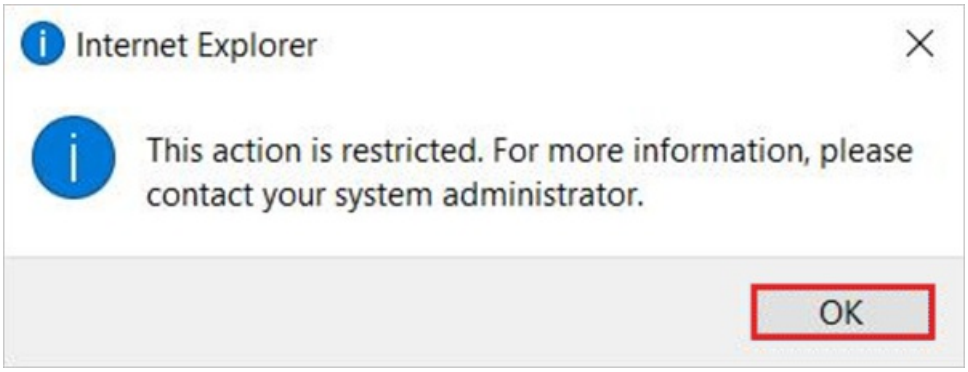
User experience after redirecting traffic to Microsoft Edge

When you enable the **Disable Internet Explorer 11 as a standalone browser** policy, all IE11 activity is

redirected to Microsoft Edge and users have the following experience:

- IE11 icons on the Start Menu and on the task bar will be removed.
- When users try to launch shortcuts or file associations that use IE11, they will be redirected to open the same file/URL in Microsoft Edge.
- When users try to launch IE11 by directly invoking the iexplore.exe binary, Microsoft Edge will launch instead.

As part of setting the policy for this experience, you can optionally show a redirect message for each user who tries to launch IE11. This message can be set to display "Always" or "Once per user". By default, the redirect message shown in the next screenshot is never shown.



If your Enterprise Mode Site List contains applications that are configured to open in the IE11 app and you disable IE11 with this policy, they will open in IE mode on Microsoft Edge.

> **NOTE**
> There was a known issue with the user flow when a site is configured to open in the IE11 application and the disable IE11 policy is set. The issue has been fixed in Microsoft Edge versions 91.0.840.0 or later.

Disable Internet Explorer 11 as a standalone browser

To disable Internet Explorer 11 using group policy, follow these steps:

1. Ensure you have the pre-requisite operating system updates. This step will update the ADMX files on your machine directly (specifically inetres.adml and inetres.admx). Please note that if you want to update your Central Store, you will need to copy over the .adml and .admx files from a machine that has the pre-requisite updates or download the latest Windows 10 Admin templates from here. For more information, see Create and manage Central Store
2. Open the Group Policy Editor.
3. Go to *Computer Configuration/Administrative Templates/Windows Components/Internet Explorer*.
4. Double-click**Disable Internet Explorer 11 as a standalone browser**.
5. Select**Enabled**.
6. Under**Options**, pick one of the following values:
   - **Never**if you don't want to notify users that IE11 is disabled.
   - **Always**if you want to notify users every time they're redirected from IE11.
   - **Once per user**if you want to notify users only the first time they are redirected.
7. Select**OK**or**Apply**to save this policy setting.

See also

- Microsoft Edge Enterprise landing page
- About IE mode
- Additional Enterprise Mode information

Enterprise Site Discovery Step-by-Step Guide

11/1/2022 • 9 minutes to read • Edit Online

> **NOTE**
>
> The retired, out-of-support Internet Explorer 11 (IE11) desktop application will be permanently disabled on certain versions of Windows 10 as part of the February 2023 Windows security update ("B") release scheduled for February 14, 2023. Learn more
>
> We highly recommend setting up IE mode in Microsoft Edge and disabling IE11 prior to this date to ensure your organization does not experience business disruption. Learn how

This article provides a step-by-step guide to using Enterprise Site Discovery with Microsoft Endpoint Configuration Manager.

> **TIP**
>
> Unless your environment requires using the steps in this guide, we recommend that you use the Microsoft Edge deployment wizard and the script it generates to configure Enterprise Site Discovery.

Enterprise Site Discovery can help you configure your Enterprise Mode Site List. Enterprise Site Discovery will help you:

- Discover which sites are using legacy document modes. Unless these sites are detecting modern browsers and providing different HTML, they probably need to use IE mode.
- Discover which sites are using ActiveX controls. Microsoft Edge doesn't support ActiveX controls. Unless these sites are detecting modern browsers and providing different HTML, they probably need to use IE mode.

> **NOTE**
>
> This article applies to Microsoft Edge **Stable**, **Beta** and **Dev** Channels, version 77 or later.

Prerequisites

This guide assumes you're experienced with using Microsoft Endpoint Configuration Manager and have the following services and roles installed:

- Microsoft Endpoint Configuration Manager
- Microsoft SQL Server Reporting Services
- (Optional) Configuration Manager Reporting Services Point Role is configured

Download Enterprise Site Discovery Tools

Download the following tools:

- Enterprise Site Discovery Setup and Configuration Package
- Microsoft Report Builder

Enable Enterprise Site Discovery

Before you can connect to Windows Management Instrumentation (WMI) to retrieve site discovery data, you need to deploy the WMI class provider to the device that's collecting this data.

From the **Enterprise Site Discovery Setup and Configuration Package**, extract the contents to a folder in your definitive software library file share. Example: **\\DSL\EnterpriseSiteDiscovery**.

Next, create a package in Microsoft Endpoint Configuration Manager, as described in Packages and programs in Configuration Manager.

Configure the new package with the following settings:

- On the **Package** page:
  - select **Name** and specify the name **Enable Site Discovery**
  - select **This package contains source files**
  - specify the source folder you extracted the files to (for example, **\\DSL\EnterpriseSiteDiscovery**)
- On the **Program Type** page, choose **Standard Program**
- On the **Standard Program** page, enter the following command to configure Site Discovery on the device:

```
powershell.exe -ExecutionPolicy Bypass .\IETelemetrySetUp-Win8.ps1
```

> **NOTE**
> The script supports using command line switches for `-ZoneAllowList` and `-SiteAllowList`. For this step-by-step, we will configure these options via group policy.

- On the **Standard Program** page:
  - select the option to run **Hidden**
  - under **Program can run**, select the option **Whether or not a user is logged in**

After creating the package, double-click on the package name **Enable Site Discovery** to view its properties. For the **After running** property, select **Configuration manager restarts computer**. WMI data collection will start after the devices reboot.

> **NOTE**
> You can configure the amount of time a user has to restart the device as described in the client settings documentation.

To confirm that data collection's working, visit a couple of websites and run the following PowerShell command to verify that data's being populated in the WMI namespace.

```
Get-WmiObject -Namespace “root/cimv2/IETelemetry” -Class IEURLInfo | Select-Object URL, NumberOfVisits,
CrashCount, DocMode | Sort-Object
```

Configure Enterprise Site Discovery via Group Policy

With Enterprise Site Discovery enabled, you can configure what data you'll collect. Consider local laws and

regulatory requirements as described in What data is collected?.

1. Open the Group Policy Editor.
2. Select **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Internet Explorer**.
3. Double-click **Turn on Site Discovery WMI output**.
4. Select **Enabled**.
5. Select **OK** or **Apply** to save this policy setting.

You can pick the zones where you want to collect site data:

1. Double-click **Limit Site Discovery output by Zone**.
2. Select **Enabled**.
3. Set the **Zone Mask** to indicate which of the following zones to enable site discovery for.

   - Restricted Sites Zone
   - Internet Zone
   - Trusted Sites Zone
   - Local Intranet Zone
   - Local Machine Zone

   > **NOTE**
   > To configure zone(s) included in site discovery, a binary number is formed based on the selected zones. The decimal representation of this number is used to represent this number in policy.

   Examples: Zone Mask 2: **00010** will collect data for the Local Intranet zone only Zone Mask 6: **00110** will collect data for Intranet and Trusted site zones only

4. Select **OK** or **Apply** to save this policy setting.

You can also limit the domains for which to collect site data:

1. Double-click **Limit Site Discovery output by domain**.
2. Select **Enabled**.
3. Enter the domains you want to collect data for, one domain per line.
4. Select **OK** or **Apply** to save this policy setting.

Collect Site Discovery data using Configuration Manager

Now that your devices are generating data, it's time to collect this data in Configuration Manager.

1. In the Configuration Manager console, choose **Administration** > **Client Settings** > **Default Client Settings**.
2. On the **Home** tab's **Properties** group, choose **Properties**.
3. In the **Default Client Settings** dialog box, choose **Hardware Inventory**.
4. In the **Device Settings** list, choose **Set Classes**.
5. In the **Hardware Inventory Classes** dialog box, choose **Add**.
6. In the **Add Hardware Inventory Class** dialog box, select **Connect**.
7. In the **Connect to Windows Management Instrumentation (WMI)** dialog box, enter the name of a computer where Enterprise Site Discovery is configured. If you're connecting to another computer, you'll need credentials with permission to access WMI.

8. In the **WMI Namespace** text box, enter **root\cimv2\IETelemetry**.
9. Choose **Connect**.
10. In the **Add Hardware Inventory Class** dialog box, in the **Inventory classes** list, select the WMI classes **IESystemINfo**, **IEUrlInfo**, and **IECountInfo**.
11. Select **OK** to close the **Class qualifiers** dialog and the other open dialogs.

After the client updates settings from the management point, data will be reported when the next hardware inventory runs (by default every seven days).

Import Site Discovery reports

The Enterprise Site Discovery package includes two sample reports. One report shows sites using ActiveX controls, and the report shows sites using legacy document modes.

Configure the Site Discovery sample report

Use the steps as a guide to create a sample report that uses three data sources. These data sources are: the sites a user visits, information about their system, and the document modes used by the sites. This report helps you identify sites that may depend on legacy document modes.

1. Copy the report **SCCM_Report-Site_Discovery.rdl** to your Configuration Manager server.
2. Install Microsoft Report Builder.
3. Double-click **SCCM_Report-Site_Discovery.rdl** to open the report in Report Builder.
4. The first time you try to open the report, it will try to contact the server where it was created. When prompted to **Connect to Report Server**, select **No**.
5. After the report opens, expand **Data Sources** and double-click **DataSource1**.
6. In the **Data Source Properties** window, select **Use a connection embedded in my report** and then select **Build...**.

> **NOTE**
> Ensure that you select Microsoft SQL Server as the Data Source. Report Builder defaults to Microsoft SQL Server Analysis Services as the data source.

7. In the **Connection Properties** window, select **Server Name** and enter the name of the Configuration Manager server. Then, in **Select or enter a database name** select the name of the Configuration Manager database from the dropdown list.
8. Select **OK** to close the **Connection Properties** window.
9. Select **Test Connection** to test the connection. If the connection's successful, select **OK** to close the **Data Source Properties** window.
10. Repeat Steps 5 through 9 for **Data Source 2**.
11. Expand **Datasets** and double-click **DataSet1**.
12. In the **Dataset Properties** window, click in the **Query:** textbox. Copy the query to Notepad and then find and replace **CM_A1B** with the database name you selected in Step 7. Paste the updated query into the **Query:** textbox.
13. Repeat steps 11 through 12 for **DataSet2**, **DataSet3**, and **DataSet4**.
14. In the **Home** tab of the ribbon, select the **Run** button to test the report.
15. Save the report and close Microsoft Report Builder.
16. Rename the report file to **Site Discovery.rdl**

Configure the ActiveX sample report

Use the following procedure to create a sample report that uses one data source: the sites that are using ActiveX

controls. Because Internet Explorer is the only browser that supports ActiveX controls, these sites may require IE mode in Microsoft Edge.

1. Copy the report **SCCM Report Sample - ActiveX.rdl** to your Configuration Manager server.
2. Install Microsoft Report Builder.
3. Double-click **SCCM Report Sample - ActiveX.rdl** to open the report in Report Builder.
4. The first time you try to open the report, it will try to contact the server where it was created. When prompted to **Connect to Report Server**, select **No**.
5. After the report opens, expand **Data Sources** and double-click **AutoGen__5C6358F2_4BB6_4a1b_A16E_8D96795D8602_**.
6. In the **Data Source Properties** window, select **Use a connection embedded in my report** and then select **Build...**.
7. In the **Connection Properties** window, select **Server Name** and enter the name of the Configuration Manager server. Then, in **Select or enter a database name** select the name of the Configuration Manager database from the dropdown list.
8. Select **OK** to close the **Connection Properties** window.
9. Select **Test Connection** to test the connection. If the connection is successful, select **OK** to close the **Data Source Properties** window.
10. Expand **Datasets** and double-click **DataSet1**.
11. In the **Dataset Properties** window, click in the **Query:** textbox. Copy the query to Notepad and then find and replace **CM_A1B** with the database name you selected in Step 7. Paste the updated query into the **Query:** textbox.
12. In the **Home** tab of the ribbon, select the **Run** button to test the report.
13. Save the report.
14. Close Microsoft Report Builder.
15. Rename the file to **ActiveX**

Upload configured reports to Microsoft SQL Server Reporting Services

After you've configured the reports for your environment, upload them to the reporting server.

1. Launch the **Reporting Services Configuration Manager** application.
2. In the **Report Server Connection** window, select **Connect** and then select the URL listed under **Web Portal Site Identification**
3. In the browser window that opens, you should be on the **SQL Server Reporting Services Page** - select the **ConfigMgr_SCCMSiteCode** folder for your SCCM Site Code.
4. In the ribbon, hover over **+New** and select the **Folder** menu item.
5. Enter a folder name, such as **Enterprise Site Discovery**, and then select the **Create** button.
6. Select the **Enterprise Site Discovery** folder.
7. On the ribbon, select the **Upload** button.
8. Select the **Site Discovery** report, and select **OK**.
9. Repeat steps 7 and 8 for the **ActiveX** report.

View reports in Configuration Manager

Now that you've customized and uploaded the reports, you can view them in Configuration Manager.

1. In the Configuration Manager console, choose **Monitoring** > **Reporting** > **Reports** > **Enterprise Site Discovery**
2. Double-click on a report to view it.

Disable Enterprise Site Discovery

When you're finished collecting data, disable Enterprise Site Discovery. Create a second package to disable Enterprise Site Discovery in Microsoft Endpoint Configuration Manager, as described in the Packages and programs in Configuration Manager. Configure the following options:

- On the **Package** page:
  - select **Name** and specify the name **Disable Site Discovery**.
  - select **This package contains source files**.
  - specify the source folder you extracted the files to (for example, **\\DSL\EnterpriseSiteDiscovery**).
- On the **Program Type** page, choose **Standard Program**.
- On the **Standard Program** page, enter the following command line to disable Site Discovery on the device:

```
powershell.exe -ExecutionPolicy Bypass .\IETelemetrySetUp-Win8.ps1 -IEFeatureOff
```

- On the **Standard Program** page:
  - select the run **Hidden** option.
  - under **Program can run**, select the option **Whether or not a user is logged in**.

See also

- Microsoft Edge Enterprise landing page
- About IE mode
- Additional Enterprise Mode information
- Additional Enterprise Site Discovery information

Enterprise Site List Manager in Microsoft Edge

11/1/2022 • 7 minutes to read • Edit Online

NOTE

The retired, out-of-support Internet Explorer 11 (IE11) desktop application will be permanently disabled on certain versions of Windows 10 as part of the February 2023 Windows security update ("B") release scheduled for February 14, 2023. Learn more

We highly recommend setting up IE mode in Microsoft Edge and disabling IE11 prior to this date to ensure your organization does not experience business disruption. Learn how

This article explains how to enable access to and use the Enterprise Site List Manager in Microsoft Edge to create, edit and export your Enterprise Mode Site List for Internet Explorer (IE) mode.

NOTE

This article applies to Microsoft Edge version 89 or later. The shared cookies capability is available on Microsoft Edge version 101 or later.

Overview

The Enterprise Site List Manager is an in-browser version of the standalone Enterprise Mode Site List Manager tool that lets you create, edit, and export your organization's site list. You can access the in-browser Enterprise Site List Manager at *edge://compat/SiteListManager*.

Future improvements to the tool for Internet Explorer mode will be available through Enterprise Site List Manager (*edge://compat/SiteListManager*) in Microsoft Edge. The standalone tool will continue to be available in the Download Center but won't get any feature updates.

Enabling access to Enterprise Site List Manager

You can configure access to the site list manager tool by using the EnterpriseModeSiteListManagerAllowed group policy.

If this policy is enabled, your users will see an option named Enterprise Site List Manager on the left navigation pane in *edge://compat*. If the policy is disabled, users won't see the entry point to Enterprise Site List Manager in the left navigation pane, which is the default behavior.

Using the Enterprise Site List Manager

The Enterprise Site List Manager tool uses the v.2 version of the schema. If you import a v.1 version schema into the Enterprise Site List Manager (schema v.2), the XML is saved into the v.2 version of the schema. See Enterprise Mode schema v.2 guidance.

Add single sites to your site list

Use the following steps to add individual sites to your site list.

> **NOTE**
> You can only add specific URLs, not Internet or Intranet Zones.

1. In the Enterprise Site List Manager, select **Add a site**.
2. Enter the URL for the website you'd like to add, for example: <domain>.com or <domain>.com/<path> in the **URL** box.
3. Select one of the following options from the **Open in** list:
   - **IE11**. Opens the site in the IE11 application.
   - **IE mode**. Opens the site in Internet Explorer mode on Microsoft Edge if enabled and in the IE11 app otherwise. See Internet Explorer mode on Microsoft Edge.
   - **MSEdge**. Opens the site in Microsoft Edge.
   - **Configurable**. Allows the site to participate in IE mode engine determination. See Configurable sites in IE mode
   - **None**. Opens in whatever browser the user chooses.
4. Under **Compat Mode**, choose one of the following options:
   - **IE8Enterprise**. Loads the site in IE8 Enterprise Mode.
   - **IE7Enterprise**. Loads the site in IE7 Enterprise Mode.
   - **IE[x]**. Where [x] is the document mode number and the site loads in the specified document mode.
   - **Default Mode**. Loads the site using the default compatibility mode for the page.

   The path within a domain can require a different compatibility mode from the domain itself. For example, the domain might look fine in the default IE11 browser, but the path might have problems and require the use of Enterprise Mode. If you added the domain previously, your original compatibility choice is still selected. However, if the domain is new, **IE8 Enterprise Mode** is automatically selected.

   Enterprise Mode takes precedence over document modes, so sites that are already included in the Enterprise Mode site list won't be affected by this update. These sites will continue to load in Enterprise Mode. For more specific information about using document modes, see Fix web compatibility issues using document modes and the Enterprise Mode site list.
5. The **Allow Redirect** checkbox applies to the treatment of server-side redirects. If you check this box, server-side redirects will open in the browser specified by the open-in tag. For more information, see `allow-redirect` in updated schema attributes.
6. Type any comments about the website into the **Comment** box. Administrators can only see comments while they're in this tool and these comments are retained in the site list xml.
7. Select **Add** to add the site to your site list.

Add shared cookies to your site list

Use the following steps to add individual shared cookies to your site list. To learn more about cookie sharing, see Cookie sharing between Microsoft Edge and Internet Explorer.

1. In the Enterprise Site List Manager, select **Add a shared cookie**.
2. Enter the domain you'd like to add in the **Domain** box. Enter the name of the cookie in the **Cookie Name** box.
3. If the cookie is a host-only cookie, then check **Host Only**.
4. If needed, enter the path in the **Path** box.

5. Select one of the following options from the **Source Engine** list:

   - **MSEdge**. Share session cookies from Microsoft Edge to Internet Explorer.
   - **IE11**. Share session cookies from Internet Explorer to Microsoft Edge.
   - **Both**. Share session cookies to and from Microsoft Edge and Internet Explorer.
6. Enter any comments about the shared cookie in the **Comment** box.
7. Select **Add** to add the shared cookie.

Export site list to XML

After you create your site list in the Enterprise Site List Manager, you can export the contents to an Enterprise Mode (.EMIE) or XML file.

> **NOTE**
> This file includes all your URLs and shared cookies and should be stored somewhere safe.

To export the site list, follow these steps:

1. In the Enterprise Site List Manager, select **Export to XML**.
2. Enter a **Version number** and a **File name**.
3. Select **Export**.

You can save the file locally or to a network share. However, you must make sure you deploy it to the location specified in your registry key. For more information, seeTurn on Internet Explorer mode and use a site list.

Import multiple sites and shared cookies to your site list

After you create your .xml file, you can bulk add sites or shared cookies to the editor using **Import from XML**.

If you want to replace all the contents in the editor, select the ellipsis (...) and then choose **Clear list**. After you clear the editor, use the following steps to import the site list.

1. In the Enterprise Site List Manager, select **Import from XML**.
2. Select **Choose file** to select your site list to add the included sites or shared cookies to the tool. Pick the site list you want to add and then select **Open**.

   Supported formats for Import are .xml, .emie, or .txt containing the v.2 schema for Enterprise Mode Site List. See Enterprise Mode schema v.2 guidance.
3. Select**Load**to add the sites or shared cookies from the file to the editor.

You can save the file locally or to a network share. However, you must make sure you deploy it to the location specified in your registry key. For more information, seeTurn on Internet Explorer mode and use a site list.

Edit sites in your site list

You can edit attributes of existing site entries in the Enterprise Site List Manager. You can also add, remove, or delete associated comments.

1. In the Enterprise Site List Manager, select the ellipsis (...) and choose **Edit site** for the URL you want to edit.
2. You can edit any attribute of the site entry except the URL. Select **Save** after you finish editing.

> **NOTE**
> If you want to delete a site entry, choose **Delete site** in step 1.

3. Select **Export to XML**, and save the updated file.

You can save the file locally or to a network share. However, you must make sure you deploy it to the location specified in your registry key. For more information, seeTurn on Internet Explorer mode and use a site list.

Edit shared cookies in your site list

You can edit attributes of existing shared cookie entries in the Enterprise Site List Manager. You can also add, remove, or delete associated comments. Use the following steps to edit shared cookies.

1. In the Enterprise Site List Manager, select the ellipsis (...) and choose **Edit cookie** for the domain you want to edit.
2. You can edit any attribute of the site entry except the Domain. Select **Save** after you finish editing.

> **NOTE**
> If you want to delete a shared cookie entry, choose **Delete shared cookie** in step 1.

Preview your site list in XML format

You can preview the sites and shared cookies in the editor in XML format before you export and save to your site list location. Select **XML preview** to open the file in a new tab.

Search in the Enterprise Site List Manager

You can search to see if a specific site or shared cookie already appears in your site list so you don't try to add it again.

To search, type part of the URL or domain into the search box in the top right-hand corner of the editor.

See also

- Microsoft Edge Enterprise landing page
- About IE mode
- Enterprise Mode schema v.2 guidance
- Additional Enterprise Mode information

Keep in-page navigation in Internet Explorer mode

11/1/2022 • 2 minutes to read • Edit Online

You can use this policy as a temporary solution to force all in-page navigation from Internet Explorer mode (IE mode) sites to stay in IE mode.

An in-page navigation is started from a link, a script, or a form on the current page. It can also be a server-side redirect of a previous in-page navigation attempt. Conversely, a user can start a navigation that isn't in-page that's independent of the current page in several ways by using the browser controls. For example, using the address bar, the back button, or a favorite link.

> **NOTE**
> This article applies to Microsoft Edge version 81 or later.

Prerequisites

The following Windows updates are required for this policy:

- Windows 11
- Windows 10 version 1909 & 1903, Windows Server version 1909 & 1903 (KB4532695)
- Windows 10 version 1809, Windows Server version 1809, Windows Server 2019 (KB4534321)
- Windows 10 version 1803 (KB4534308)
- Windows 10 version 1709 (KB4534318)

About this policy

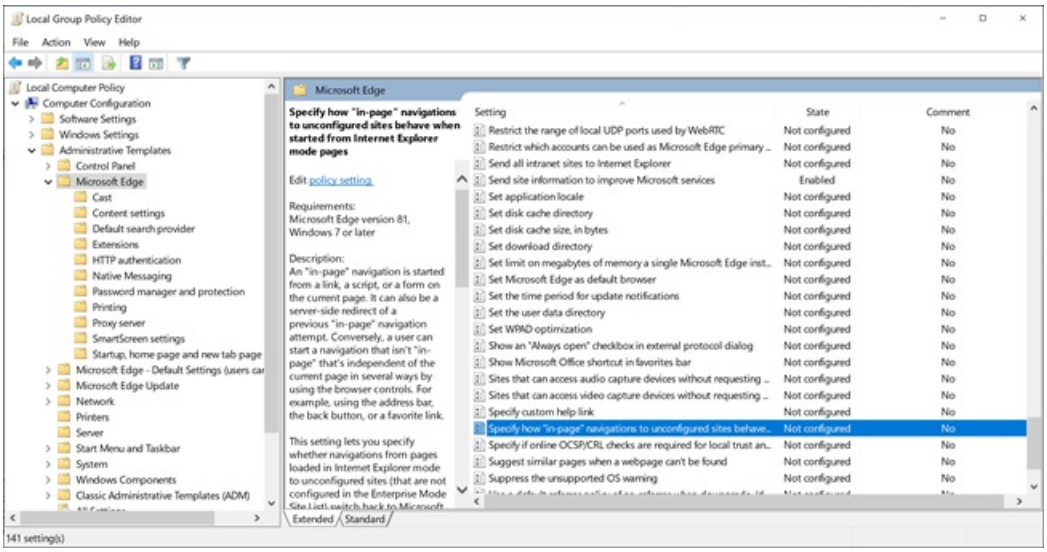
This policy gives you time to identify and configure all of the authentication servers used by your IE mode sites. However, this policy can result in an inconsistent browsing experience, where some sites are rendered in IE mode and at other times rendered in Microsoft Edge mode. This experience depends on whether the navigation to the site began from an IE mode page. Any site that isn't explicitly configured to open in a specific rendering engine will be subject to this inconsistency.

If you enable this policy, we recommend that you disable it after you've identified all the authentication servers and added them to the site list as neutral. This action ensures that your modern sites never inadvertently render in IE mode.

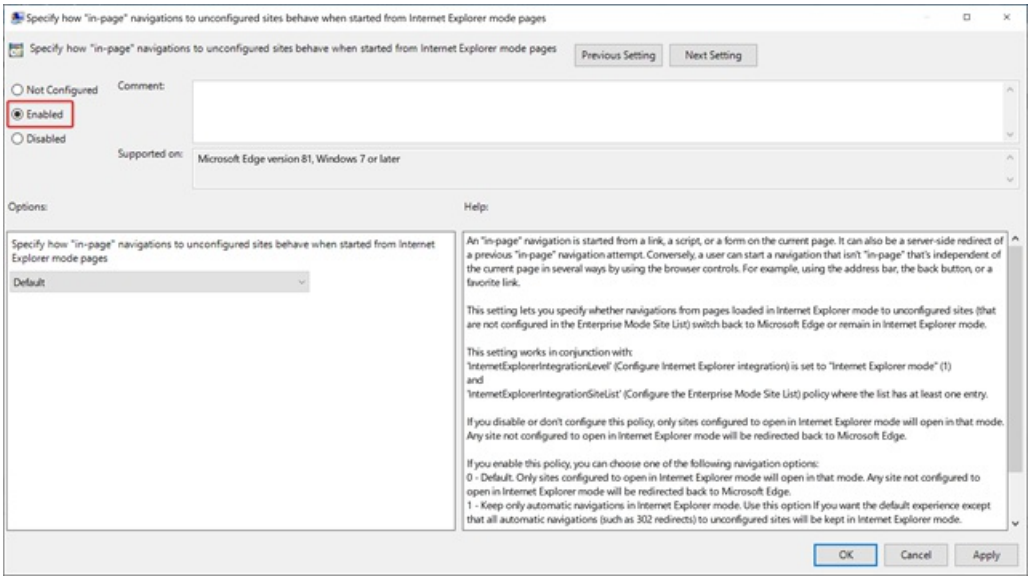
Keep in-page navigation in IE mode

To keep automatic or all in-page navigation in Internet Explorer mode, follow these steps:

1. Open Local Group Policy Editor.
2. Click **Computer Configuration** > **Administrative Templates** > **Microsoft Edge**.
3. Under **Setting**, double-click **Specify how "in-page" navigations to unconfigured sites behave when started from Internet Explorer mode pages**.


Local Group Policy Editor
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
Control Panel
Microsoft Edge
Cast
Content settings
Default search provider
Extensions
HTTP authentication
Native Messaging
Password manager and protection
Printing
Proxy server
SmartScreen settings
Startup, home page and new tab page
Microsoft Edge - Default Settings (users can
Microsoft Edge Update
Network
Printers
Server
Start Menu and Taskbar
System
Windows Components
Classic Administrative Templates (ADM)
Microsoft Edge
Specify how "in-page" navigations to unconfigured sites behave when started from Internet Explorer mode pages
Edit policy setting
Requirements:
Microsoft Edge version 81, Windows 7 or later
Description:
An "in-page" navigation is started from a link, a script, or a form on the current page. It can also be a server-side redirect of a previous "in-page" navigation attempt. Conversely, a user can start a navigation that isn't "in-page" that's independent of the current page in several ways by using the browser controls. For example, using the address bar, the back button, or a favorite link.
This setting lets you specify whether navigations from pages loaded in Internet Explorer mode to unconfigured sites (that are not configured in the Enterprise Mode
Setting
State
Comment
Restrict the range of local UDP ports used by WebRTC
Restrict which accounts can be used as Microsoft Edge primary ...
Send all intranet sites to Internet Explorer
Send site information to improve Microsoft services
Set application locale
Set disk cache directory
Set disk cache size, in bytes
Set download directory
Set limit on megabytes of memory a single Microsoft Edge inst...
Set Microsoft Edge as default browser
Set the time period for update notifications
Set the user data directory
Set WPAD optimization
Show an "Always open" checkbox in external protocol dialog
Show Microsoft Office shortcut in favorites bar
Sites that can access audio capture devices without requesting ...
Sites that can access video capture devices without requesting ...
Specify custom help link
Specify how "in-page" navigations to unconfigured sites behave...
Specify if online OCSP/CRL checks are required for local trust an...
Suggest similar pages when a webpage can't be found
Suppress the unsupported OS warning
Not configured
Enabled
No
Extended
Standard
141 setting(s)

4. Select **Enabled**


Specify how "in-page" navigations to unconfigured sites behave when started from Internet Explorer mode pages
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
Microsoft Edge version 81, Windows 7 or later
Options:
Help:
Default
An "in-page" navigation is started from a link, a script, or a form on the current page. It can also be a server-side redirect of a previous "in-page" navigation attempt. Conversely, a user can start a navigation that isn't "in-page" that's independent of the current page in several ways by using the browser controls. For example, using the address bar, the back button, or a favorite link.
This setting lets you specify whether navigations from pages loaded in Internet Explorer mode to unconfigured sites (that are not configured in the Enterprise Mode Site List) switch back to Microsoft Edge or remain in Internet Explorer mode.
This setting works in conjunction with:
'InternetExplorerIntegrationLevel' (Configure Internet Explorer integration) is set to "Internet Explorer mode" (1)
and
'InternetExplorerIntegrationSiteList' (Configure the Enterprise Mode Site List) policy where the list has at least one entry.
If you disable or don't configure this policy, only sites configured to open in Internet Explorer mode will open in that mode. Any site not configured to open in Internet Explorer mode will be redirected back to Microsoft Edge.
If you enable this policy, you can choose one of the following navigation options:
0 - Default. Only sites configured to open in Internet Explorer mode will open in that mode. Any site not configured to open in Internet Explorer mode will be redirected back to Microsoft Edge.
1 - Keep only automatic navigations in Internet Explorer mode. Use this option if you want the default experience except that all automatic navigations (such as 302 redirects) to unconfigured sites will be kept in Internet Explorer mode.
OK
Cancel
Apply

5. Choose one of the following options from the dropdown list:

   - **Default** - Only sites configured to open in Internet Explorer mode will open in that mode. Any site not configured to open in Internet Explorer mode will be redirected back to Microsoft Edge.
   - **Keep only automatic navigations in Internet Explorer mode** - Use this option if you want the default experience except that all automatic navigations (such as 302 redirects) to unconfigured sites will be kept in Internet Explorer mode.
   - **Keep all in-page navigation in Internet Explorer mode** ***(Least Recommended)*** - All navigations from pages loaded in IE mode to unconfigured sites are kept in Internet Explorer mode.

6. Click **OK** or **Apply** to save the policy settings.

See also

- Microsoft Edge Enterprise landing page

Cookie sharing between Microsoft Edge and Internet Explorer

11/1/2022 • 4 minutes to read • Edit Online

NOTE

The retired, out-of-support Internet Explorer 11 (IE11) desktop application will be permanently disabled on certain versions of Windows 10 as part of the February 2023 Windows security update ("B") release scheduled for February 14, 2023. Learn more

We highly recommend setting up IE mode in Microsoft Edge and disabling IE11 prior to this date to ensure your organization does not experience business disruption. Learn how

This article explains how to configure session cookie sharing between a Microsoft Edge process and an Internet Explorer process, while using Internet Explorer mode.

NOTE

This article applies to Microsoft Edge version 87 or later.

Prerequisites

To share session cookies from Microsoft Edge to Internet Explorer:

- Windows updates
  - Windows 11
  - Windows 10 version 2004, Windows Server version 2004 - KB4571744 or higher
  - Windows 10 version 1909, Windows Server version 1909 – KB4566116 or higher
  - Windows 10 version 1903, Windows Server version 1903 – KB4566116 or higher
  - Windows 10 version 1809, Windows Server version 1809, and Windows Server 2019 - KB4571748 or higher
  - Windows 10 version 1803 – KB4577032 or higher
  - Windows 10 Enterprise 2016 LTSC and Windows Server 2016 - KB4580346 or higher
  - Windows 10 Enterprise 2015 LTSB - KB4580327 or higher
  - Windows 8.1 and Windows Server 2012 R2 - KB4586768 or higher
  - Windows 10 Enterprise 2016 LTSC and Windows Server 2016 - KB4580346 or higher
  - Windows 10 Enterprise 2015 LTSB - KB4580327 or higher
  - Windows 8.1 and Windows Server 2012 R2 - KB4586768 or higher
- Microsoft Edge version 87 or later
- IE modeconfigured with Enterprise Mode Site List

To share session cookies between Microsoft Edge and Internet Explorer:

- Windows updates
  - Windows 11 - KB5010414 or higher
  - Windows Server 2022 - KB5010421 or higher

- Windows 10 version 20H2 - KB5010415 or higher
- Windows 10 version 21H1 - KB5010415 or higher
- Windows 10 version 21H2- KB5010415 or higher

- Microsoft Edge version 99 or later
- IE modeconfigured with Enterprise Mode Site List

Overview

A common configuration in large organizations is to have an application that works on a modern browser link to another application, which might be configured to open in Internet Explorer mode with Single Sign On (SSO) enabled as part of the workflow.

By default, the Microsoft Edge and Internet Explorer processes don't share session cookies, and this lack of sharing can be inconvenient in some cases. For example, when a user has to reauthenticate in Internet Explorer mode or when signing out of a Microsoft Edge session doesn't sign out of the Internet Explorer mode session. In these scenarios, you can configure specific cookies set by SSO to be sent from Microsoft Edge to Internet Explorer so the authentication experience becomes more seamless by eliminating the need to reauthenticate.

> **NOTE**
> Before Microsoft Edge version 99, session cookies can only be shared from Microsoft Edge to Internet Explorer. Starting with Microsoft Edge version 99, sharing session cookies in reverse (from Internet Explorer to Microsoft Edge) is possible.

> **NOTE**
> Persistent cookies, which have been created with an Expires-attribute, are not in scope for this feature and cannot be shared between Microsoft Edge and Internet Explorer.

How cookie sharing works

The Enterprise Mode site list XML is extended to allow more elements to specify session cookies that need to be shared between Microsoft Edge and Internet Explorer.

The first time an Internet Explorer mode tab is created in a Microsoft Edge session, all matching cookies are shared to the Internet Explorer session. After that, anytime a cookie that matches a rule is added, deleted, or modified it's sent as an update to the Internet Explorer session. The set of shared cookies is also reevaluated when the site list is updated.

Updated schema elements

The following table describes the <shared-cookie> element added to support the cookie sharing feature.

ELEMENT	DESCRIPTION

ELEMENT	DESCRIPTION
<shared-cookie **domain**=".contoso.com" **name**="cookie1"> </shared-cookie> OR <shared-cookie **host**="subdomain.contoso.com" **name**="cookie2"> </shared-cookie>	**(Required)** A <shared-cookie> element requires, at minimum, a *domain* (for domain cookies) or a *host* (for host-only cookies) attribute and a *name* attribute. These attributes must be exact matches to the cookie's domain and name respectively. **Note** that subdomains do not match. The *domain* attribute is used for domain cookies (and a leading dot is allowed but optional). The *host* attribute is used for host-only cookies (and a leading dot is an error). Specifying neither or both will result in an error. * A cookie is a domain cookie if a domain was specified in the cookie string (via HTTP Set-Cookie response header or document.cookie JS API). A domain cookie applies to the specified domain and all subdomains. If a domain wasn't specified in the cookie string, the cookie is a host-only cookie and only applies to the specific host that it was set for. Some classes of URLs such as single-word hostnames (for example, http://intranetsite) and IP addresses (for example, http://10.0.0.1) can only set host-only cookies.
<shared-cookie **host**="subdomain.contoso.com" **name**="cookie2" **path**="/a/b/c"> </shared-cookie>	**(Optional)** A *path* attribute may be specified. If no path attribute is specified (or if the path attribute is empty), any cookies matching domain/host and name match the policy, regardless of path (wildcard rule). If a path is specified, it must be an exact match. If a cookie matches a rule with a path, that takes precedence over a rule without a path.
<shared-cookie **domain**=".contoso.com" **name**="cookie1" **source-engine**="MSEdge"> </shared-cookie> OR <shared-cookie **domain**=".contoso.com" **name**="cookie1" **source-engine**="IE11"> </shared-cookie> OR <shared-cookie **domain**=".contoso.com" **name**="cookie1" **source-engine**="Both"> </shared-cookie>	**(Optional)** The source-engine attribute specifies how the session cookies are shared between Microsoft Edge and Internet Explorer. Where: - **MSEdge**. Share session cookies from Microsoft Edge to Internet Explorer. - **IE11**. Share session cookies from Internet Explorer to Microsoft Edge. - **Both**. Share session cookies to and from Microsoft Edge and Internet Explorer. - **Default or not specified**. Session cookies will be shared from Microsoft Edge to Internet Explorer.

Sharing example

```
<site-listversion="1">
<shared-cookiedomain=".contoso.com"name="cookie1"></shared-cookie>
<shared-cookiehost="subdomain.contoso.com"name="cookie2"path="/a/b/c">
</shared-cookie>
<shared-cookie host="subdomain.contoso.com" name="cookie3" source-engine="MSEdge"></shared-cookie>
</site-list>
```

See also

- About IE mode
- Configurable sites information
- Additional Enterprise Mode information

- Microsoft Edge Enterprise landing page

Learn about Configurable sites in IE mode

11/1/2022 • 3 minutes to read • Edit Online

This article explains the Configurable sites feature of the Enterprise Mode Site List when using IE mode in Microsoft Edge.

Prerequisites

- Windows updates
  - Windows 11
  - Windows 10 version 1909, Windows server version 1909 – KB4550945 or higher
  - Windows 10 version 1903, Windows server version 1903 – KB4550945 or higher
  - Windows 10 version 1809, Windows Server version 1809, and Windows Server 2019 - KB4550969 or higher
  - Windows 10 version 1803 – KB4550944 or higher
  - Windows 10 version 1607, Windows Server 2016 - KB4556826 or higher
  - Windows 10 initial version, July 2015 - KB4550947 or higher
  - Windows 8.1 – KB4556798 or higher
- Microsoft Edge version 83 or later
- IE mode configured with Enterprise Mode Site List

Overview

Configuring sites needing IE mode in the Enterprise Mode Site List will work well for most environments with legacy applications. However, in some cases this approach isn't the best to configure a subset of sites to open in IE mode without rendering an entire domain in IE mode. For example, when your environment contains both modern and legacy applications running on a single server and you would like the flexibility to render only the legacy applications in IE mode and the remaining applications to render in Microsoft Edge mode.

The solution is to use the Configurable sites feature of the Enterprise Mode Site List. When the feature is enabled, Microsoft Edge will allow sites with the "configurable" tag to participate in IE mode engine determination.

How Configurable sites works

Automatic switching from the Microsoft Edge engine to the IE mode engine

To use the Configurable sites feature, you'll need one or more sites in the Enterprise Mode Site List to have the `<open-in>Configurable</open-in>` option.

Example:

```
<site-list version="1">
 <site url="app.com">
 <open-in>Configurable</open-in>
 </site>
</site-list>
```

When the Configurable sites feature is enabled, the following behavior occurs:

1. When making a request to a Configurable site, Microsoft Edge will send the HTTP request header "`X-InternetExplorerModeConfigurable: 1`".
2. A Configurable site may send a redirect response (for example, HTTP 302) with the HTTP response header "`X-InternetExplorerMode: 1`" to request that Microsoft Edge loads the site in IE mode.
3. The target of the redirect (that is, the value of the **Location** response header) must also be a **Configurable** or **Neutral** site, otherwise the IE mode response header will be ignored. It's expected that the target of the redirect will usually be the same as the original URL. However, it doesn't have to be.

   > **NOTE**
   > The redirect response is subject to caching according to Microsoft Edge's normal HTTP caching behavior for redirects.

Switching back from IE mode engine to Microsoft Edge engine

Enabling Configurable sites in Microsoft Edge automatically enables the following behaviors in IE mode tabs:

1. When making a request to a Configurable site, IE mode tabs will send the HTTP request header "`X-InternetExplorerModeConfigurable: 1`", the same as Microsoft Edge tabs.
2. A Configurable site might send a redirect response (for example, HTTP 302) with the HTTP response header "`X-InternetExplorerMode: 0`" to request that the navigation switch back to Microsoft Edge mode.
3. The target of the redirect (that is, the value of the **Location** response header) must also be a **Configurable** or **Neutral** site, otherwise the IE mode response header will be ignored. It's expected that the target of the redirect will usually be the same as the original URL. However, it doesn't have to be.

   > **NOTE**
   > The redirect response is subject to caching according to Microsoft Edge's normal HTTP caching behavior for redirects.

> **TIP**
> Both browser engines send the same "`X-InternetExplorerModeConfigurable: 1`" request header to Configurable sites. You should use the User-Agent request header to distinguish between requests from Microsoft Edge mode vs. IE mode to avoid redirecting when the site is already loading in the correct engine.

See also

- About IE mode
- Additional Enterprise Mode information
- Microsoft Edge Enterprise landing page

Associate file extensions with Internet Explorer mode

11/1/2022 • 2 minutes to read • Edit Online

> **NOTE**
>
> The retired, out-of-support Internet Explorer 11 (IE11) desktop application will be permanently disabled on certain versions of Windows 10 as part of the February 2023 Windows security update ("B") release scheduled for February 14, 2023. Learn more
>
> We highly recommend setting up IE mode in Microsoft Edge and disabling IE11 prior to this date to ensure your organization does not experience business disruption. Learn how

This article explains how to associate Microsoft Edge with Internet Explorer mode with file extensions for desktop applications.

> **NOTE**
>
> This article applies to Microsoft Edge version 86 or later.

Guidance for file extension association with Internet Explorer mode

The following instructions show an entry that associates Microsoft Edge with IE mode with the .mht file type. Use the following steps as a guide for setting a file association.

> **NOTE**
>
> You can set specific file extensions to open in Internet Explorer mode by default using the policy to **Set a default associations configuration file**. For more information, see Policy CSP - ApplicationDefaults.

1. Define a new ProgID with the Microsoft Edge channel to use to open with Internet Explorer mode. The ProgID includes the application name and Icon and the full path to msedge.exe.

```
[HKEY_CURRENT_USER\SOFTWARE\Classes\MSEdgeIEModeMHT\Application]
"ApplicationCompany"="Microsoft Corporation"
"ApplicationName"="Microsoft Edge with IE Mode"
"ApplicationIcon"="C:\\<edge_installation_dir>\\msedge.exe,0"
"AppUserModelId"=""
```

```
[HKEY_CURRENT_USER\SOFTWARE\Classes\MSEdgeIEModeMHT\DefaultIcon]
@="C:\\<edge_installation_dir>\\msedge.exe,4"
```

2. Configure shell updates to pass the command line needed to open with IE mode.

```
[HKEY_CURRENT_USER\SOFTWARE\Classes\MSEdgeIEModeMHT\shell\open\command]
@="\"C:\\<edge_installation_dir>\\msedge.exe\" -ie-mode-file-url -- \"%1\""
```

3. Finally, associate the .mht file extension with a new ProgID. Add your ProgID as a value name, with the value type of REG_SZ.

```
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.mht\OpenWithProgids]
"MSEdgeIEModeMHT"=hex(0):
```

After you set the keys described in the previous example, your users will see another option on the **Open with** menu to open an .mht file using Microsoft Edge <channel> with IE mode.

Registry Example

You can save the following code snippet as a .reg file and import it into the registry.

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.mht\OpenWithProgids]
"MSEdgeIEModeMHT"=hex(0):

[HKEY_CURRENT_USER\SOFTWARE\Classes\MSEdgeIEModeMHT]

[HKEY_CURRENT_USER\SOFTWARE\Classes\MSEdgeIEModeMHT\Application]
"ApplicationCompany"="Microsoft Corporation"
"ApplicationName"="Microsoft Edge with IE Mode"
"ApplicationIcon"="C:\\<edge_installation_dir>\\msedge.exe,0"
"AppUserModelId"=""

[HKEY_CURRENT_USER\SOFTWARE\Classes\MSEdgeIEModeMHT\DefaultIcon]
@="C:\\<edge_installation_dir>\\msedge.exe,4"

[HKEY_CURRENT_USER\SOFTWARE\Classes\MSEdgeIEModeMHT\shell]

[HKEY_CURRENT_USER\SOFTWARE\Classes\MSEdgeIEModeMHT\shell\open]

[HKEY_CURRENT_USER\SOFTWARE\Classes\MSEdgeIEModeMHT\shell\open\command]
@="\"C:\\<edge_installation_dir>\\msedge.exe\" -ie-mode-file-url -- \"%1\""
```

Configuring file types to open in Internet Explorer mode

Starting with Microsoft Edge 88, you can configure specific file type links to open in Internet Explorer mode using the policy Show context menu to open links in Internet Explorer mode.

You can define file types this option should apply to, by specifying file extensions in this policy Open local files in Internet Explorer mode file extension allow list.

See also

- About IE mode
- Configurable sites information
- Additional Enterprise Mode information
- Setting file type associations
- Microsoft Edge Enterprise landing page

Internet Explorer (IE) mode troubleshooting and FAQ

11/1/2022 • 19 minutes to read • Edit Online

NOTE

The retired, out-of-support Internet Explorer 11 (IE11) desktop application will be permanently disabled on certain versions of Windows 10 as part of the February 2023 Windows security update ("B") release scheduled for February 14, 2023. Learn more

We highly recommend setting up IE mode in Microsoft Edge and disabling IE11 prior to this date to ensure your organization does not experience business disruption. Learn how

This article provides troubleshooting tips and FAQ for Microsoft Edge version 77 or later.

NOTE

This article applies to Microsoft Edge version 77 or later.

What if I need help with setting up Microsoft Edge or Internet Explorer mode?

We offer various support options. If you have Microsoft Unified Support, you can reach out to that support service for help with the transition. There's alsoFastTrack, available at no extra charge to customers with 150 or more paid seats of Windows 10.

We also recommend our Microsoft Edge + Internet Explorer mode Getting Started guide and our IE mode blog series.

Are there any tools that I can use to guide me through IE mode troubleshooting?

Yes, the Microsoft Virtual Agent provides a scenario-based guided walkthrough for troubleshooting IE mode.

There's also the next video, which provides IE mode troubleshooting tips and tricks.

.

Common IE mode issues

Use this section as a guide to help you troubleshoot and fix the two most common issues when moving to Microsoft Edge with IE mode. These issues are:

- Incorrect Document mode configurations
- Incomplete neutral site configurations

Incorrect Document mode configurations

This section describes the symptoms and gives steps to diagnose and fix this issue.

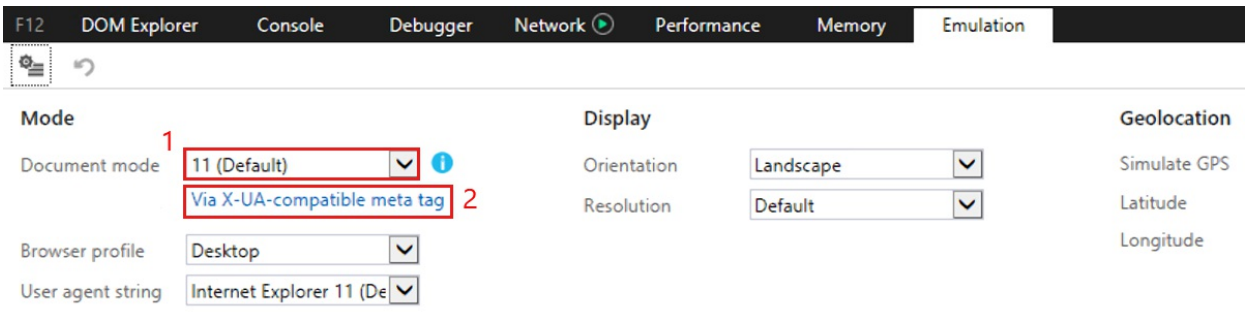
Symptoms

Users will experience the following symptoms:

- Sizing and positioning of page elements might be off or they might be missing
- Some functionality might be lost or not work as expected. For example, buttons that worked with Internet Explorer don't do anything or return an error.

How to troubleshoot and fix

The general strategy is to duplicate the same settings that worked with Internet Explorer 11 for a specific site in our IE mode site list. Use the F12 Developer Toolbar's "Emulation" tab in IE 11, shown in the next screenshot to investigate the scenario you want to fix. To open the Developer toolbar, press the F12 key and then select **Open DevTools**.



The Emulation tab shows two pieces of information to focus on: the Document mode (1), and the text below the dropdown list (2). This information can help explain why we are in the 11 (Default) mode for the page or site we're looking at.

There are different messages that can be displayed for the Document mode, and in our example they are:

- Via X-UA-compatible meta tag
- Via X-UA-compatible HTTP header

The two X-UA-Compatible options indicate that either the webpage or the web server where the site is hosted is showing the document mode that should be used by the browser.

We want to honor the document mode in nearly all cases. To do that, we need to select one of the following modes in the IE mode site list entry for the site:

- Default
- IE8 Enterprise
- IE7 Enterprise

These options respect the webpage or web server directives. Remember that we need to select an option that includes the specified document mode. In the screenshot example, because the specified document mode is 11, we'd select "Default" because IE8 Enterprise and IE7 Enterprise don't support IE 11 document mode.

If the Document mode indicates that one of the following compatibility views is needed for the site, the configuration setting is straightforward.

- Via local compatibility view settings
- Via the compatibility view list
- Via intranet compatibility settings

Because all the Compatibility View settings result in "IE7 Enterprise" behavior, choose this setting in the "Compat Mode" section of the IE mode site list entry.

For more information about the logic that Internet Explorer or IE mode uses to land in one doc mode over another, see the Deprecated document modes and Internet Explorer 11 article.

The general rule is to use the most current logic-based mode that allows a given site to work as expected. We'd start with the Default mode, move to IE8 Enterprise mode, and then to IE7 Enterprise mode if needed. This selection gives child pages the flexibility to use different Document modes as necessary via the built-in logic for their specific needs. As a result, all the website pages aren't locked in to one specific Document mode.

The following table lists the available document modes for these settings.

LOGIC-BASED MODE	DEFAULT	IE8 ENTERPRISE	IE7 ENTERPRISE
Available Document modes	IE11 Doc mode IE10 Doc mode IE9 Doc mode IE8 Doc mode IE7 Doc mode IE5 Quirks mode	IE8 Doc mode IE7 Doc mode IE5 Quirks mode	IE7 Doc mode IE5 Quirks mode

> **NOTE**
> In some cases, a particular site or page requires a specific document mode to function as designed. We recommend that explicit Document mode options should only be used when the logic-based options aren't effective.

Incomplete neutral site configurations

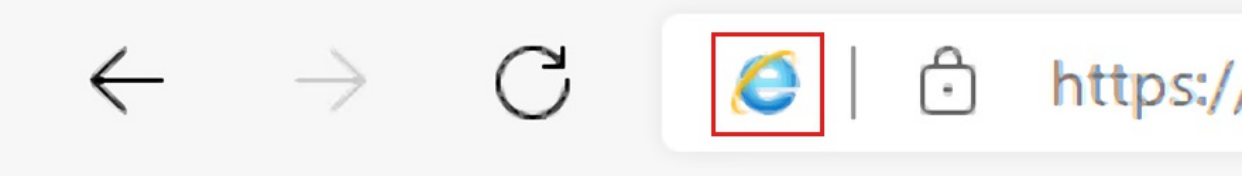
This section describes the symptoms and gives steps to diagnose and fix this issue.

Symptoms

A page relies on SSO for authentication, but users are prompted multiple times for credentials, experience a looping redirect behavior, failed authentication errors, or some combination of these symptoms.

How to troubleshoot and fix

Before we start analyzing a failing workflow in Microsoft Edge, look at the address bar for the IE mode "e" logo, shown in the next screenshot.



If, during the SSO authentication process, we see the "e", but it disappears after a redirect, this behavior points to a missing neutral site. After Microsoft Edge drops into IE mode, we need to stay there to maintain session and cookie information. If the URL shows up in the address bar long enough to identify it, add it to the IE mode site list as a neutral site using the steps described in Configure neutral sites.

Often, the redirect cycle happens so quickly that it's difficult to identify the missing neutral sites. To help with this analysis, we use a tool that's built into the Chromium engine: **net-export**.

> **TIP**
> Network traces are inherently noisy. To minimize the noise, close all other browser instances and tabs that aren't needed for the specific workflow that you're investigating.

The following steps describe how to troubleshoot a neutral site configuration.

1. Open a new tab in Microsoft Edge and go to *edge://net-export*.
2. Select **Start Logging to Disk**, and then pick a location where you want to save the resulting .json log. This log can safely be deleted after you finish troubleshooting.
3. Open another tab (keep the net-export tab open), and repeat the failing workflow.
4. After you finish, return to the net-export tab and select **Stop Logging**.
5. Select the "netlog viewer" hyperlink.
6. On the resulting page, select **Choose File**, and then pick the .json file you created in step 2.
7. After the log file is loaded, select **Events** from the left side menu.
8. Scroll through the network log and identify the starting URL. (You can also use the search function to find your starting point.)
9. From the starting point, scroll downward and look for URLs in the workflow that don't have an entry in your IE mode site list. Pay special attention to URLs with indicators for SSO, AUTH, LOGIN, and so on.
10. After you identify a candidate URL, add it to the IE mode site list as a neutral site by selecting **None** in the Open-in dropdown. Test the workflow again.

In some cases, multiple neutral site entries are needed, depending on the specific site architecture in place. If the workflow still fails after adding a new neutral site, repeat the process to capture a new net-export log and perform another pass.

In some rare instances, it may be necessary to configure specific shared cookies to ensure that required information gets to your IE mode sites. If you're aware of a specific cookie that's needed, you can configure cookie sharing using the steps described in Cookie sharing from Microsoft Edge to Internet Explorer.

What if these steps don't fix the issue?

This article is designed to help troubleshoot the most common IE mode configuration issues, but it might not cover every possible scenario. If you run into an issue that you can't fix and need help with, contact App Assure

at https://aka.ms/AppAssure and we'll help you with your problem.

Get general diagnostic and configuration information

You can get Internet Explorer mode diagnostic information on the Microsoft Edge Compatibility tab. To open this tab, go to *edge://compat/iediagnostic*. The "Internet Explorer mode diagnostic information" page might show diagnostic messages and you can export diagnostic data to an xml file. This diagnostic information page also provides configuration information for the following categories:

- **Registry key check.** (Displayed only if the check fails.) Checks to see if Internet Explorer integration is set up correctly in the registry. If not, the user can select **Fix it** to resolve the problem.
- **Internet Explorer mode.** Shows the API version that's used, based on the configuration and OS. If there's a problem, the user may be prompted to install a Windows Update.
- **Internet Explorer mode setting.** Shows whether Internet Explorer mode is enabled, and how it's configured.
- **Command line.** Shows the command-line string and switches used to start Microsoft Edge.
- **Group policy settings.** Shows whether IE mode is configured using group policies, and the policies that are applied.

Error message: "To open this page in Internet Explorer mode, reinstall Microsoft Edge with administrator privileges."

You might see this error if you don't have all required Windows Updates. See the prerequisites listed in About IE mode for the required versions of Windows and Microsoft Edge.

If you've already installed all required Windows Updates, you might see this error if:

- You're using the Canary channel, which is installed at the user level by default.
- You're using the Stable, Beta, or Dev channel, but when prompted for elevation when installing the elevation was canceled. When you cancel the elevation prompt, the installation will continue at the user level.
- Internet Explorer 11 has been disabled in Windows Features.

Possible solutions are:

- Run the installer for any channel at the system level: `installer.exe --system-level`.
- Enable Internet Explorer 11 in Windows Features.

To check if Microsoft Edge is installed at the systems level, type "edge://version" in the Microsoft Edge address bar. The Executable path will show a path starting with *C:\Program Files*, which indicates a system install. If the Executable path begins with *C:\Users*, uninstall and then reinstall Microsoft Edge with administrator privileges.

Error message "To open this page in IE mode, try restarting Microsoft Edge."

You might see this error if there was an unexpected error in Internet Explorer. Restarting Microsoft Edge usually fixes this error.

Error message: "Turn off remote debugging to open this site in IE mode otherwise it might not work as expected."

You might see this error if you're remote debugging and navigate to a web page configured to run in IE mode. You can continue, but the page will be rendered using Microsoft Edge.

Error message: "Could not retrieve EMIE site list."

You might see this error on the *edge://compat/enterprise* page indicating that the site list download failed. Starting with Microsoft Edge version 87, when cookies are blocked for third party requests using the BlockThirdPartyCookies policy, HTTP authentication also isn't allowed. You can allow cookies for the specific domain hosting your Enterprise Mode Site List using the CookiesAllowedForURLs policy to ensure that site list downloads are successful.

Error message: "The connection for this site is not secure"

This error may happen if you're trying to open a legacy website in IE mode and the site's configured to run in TLS 1.0 or TLS 1.1. These protocols are disabled by default in Microsoft Edge. For more information, see Plan for change: TLS 1.0 and TLS 1.1 soon to be disabled by default

Error message: "This form cannot be opened in a web browser. To open this form, use Microsoft InfoPath"

Certain applications may require you to load the web page in IE mode. You can use the IE mode feature in Microsoft Edge.

You may also have to set the `compat-mode` attribute in Enterprise Mode Site List to **Default**. For more information, see Enterprise Mode and the Enterprise Mode Site List.

> **TIP**
> Your users can easily view this site list and the compatibility mode by typing **about:compat** in Microsoft Edge.

Frequently Asked Questions

Will IE mode replace Internet Explorer 11?

Yes. The retired, out-of-support Internet Explorer 11 (IE11) desktop application will be permanently disabled on certain versions of Windows 10 as part of the February 2023 Windows security update ("B") release scheduled for February 14, 2023. Learn more

We highly recommend setting up IE mode in Microsoft Edge and disabling IE11 prior to this date to ensure your organization does not experience business disruption. Learn how

Can I use "View in File Explorer" in SharePoint Online on Microsoft Edge?

Starting with Microsoft Edge version 95, you can enable the **View in File Explorer** capability for SharePoint Online Modern Document Libraries. For this experience to be visible and work for your users, you'll need to enable the Microsoft Edge "Configure the View in File Explorer feature for SharePoint pages in Microsoft Edge" policy and update your SharePoint Online tenant configuration. Learn more: View SharePoint files with File Explorer in Microsoft Edge - SharePoint in Microsoft 365 | Microsoft Docs.

However, rather than use the View in File Explorer option, the recommended approach to managing files and folders outside of SharePoint is to Sync SharePoint and Teams files with your computer or Move or copy files in SharePoint.

Does IE mode on Microsoft Edge support the 'no-merge' option that was supported in Internet Explorer 11?

The recommended alternatives for the no-merge functionality in Microsoft Edge are one of the following actions:

1. Use Profiles in Microsoft Edge - Each profile maps to a different IE session for IE mode pages, so it behaves identically to the no-merge option.
2. Use the `--user-data-dir=<path>` command line, but with a different path for each session. If needed, you can create a utility for the user to run that launches Microsoft Edge and changes the path for the session.

If neither of the previous options work for your scenario, starting in Microsoft Edge version 93, IE mode on Microsoft Edge will support no-merge. For an end user, when a new browser window is launched from an IE mode application, it will be in a separate session, like the no-merge behavior in IE11.

For each Microsoft Edge window, the first time an IE mode tab is visited within that window, if it's a designated "no-merge" site, that window is locked into a different "no-merge" IE session. This window stays locked from all other Microsoft Edge windows until the last IE mode tab is closed in the locked window. This follows previous behavior where users could launch IE with no-merge and launch Microsoft Edge without no-merge using other

mechanisms. All sites opening in a new window (through window.open) will respect the merge nature of the parent process.

> **NOTE**
> Session switching isn't supported. Navigations within the same IE mode tab will use the same session.

> **NOTE**
> Sharing cookies from IE mode to Microsoft Edge mode is not supported in no-merge IE mode sessions.

You can validate the no-merge behavior in Microsoft Edge version 93 or later by following these steps:

1. Ensure that IE mode is enabled on Microsoft Edge version 93 or later.
2. You can configure sites that need to prevent session sharing in the Enterprise Mode Site List by setting the value of the merge-type attribute to "no-merge". This attribute is not applicable only when the open-in element is set to Microsoft Edge. By default, all sites have a merge-type value of merge. (**Note:** The integrated site list manager tool available at *edge://compat/sitelistmanager* includes a **No merge** checkbox when you Add or Edit a site.)

   ```
   <site url="contoso.com">
   <open-in merge-type="no-merge">IE11</open-in>
   </site>
   ```

3. Navigate to any site configured as no-merge. The site should be in its own unmerged IE session. When you open another Microsoft Edge instance or window and navigate to the same site, it should be in its own IE session. Note that there are multiple iexplore.exe processes in Task Manager.

If you have any feedback, reach out through one of our feedback channels: Microsoft support or the TechCommunity forum.

Can I save links as webpages in Internet Explorer mode?

Yes, you can enable the Save Target As option in the context menu for Internet Explorer mode in Microsoft Edge. To do this, configure the group policy "*Allow Save Target As in Internet Explorer mode*" located at **Computer Configuration > Administrative Templates > Windows Components > Internet Explorer**. The save mechanism works the same as it does in Internet Explorer and if the target is saved as an html file, reopening the file will render the page in Microsoft Edge.

The ability to save links as web pages requires the following minimum operating system updates:

- Windows 10, version 2004, Windows Server version 2004, Windows 10, version 20H2 : KB4580364
- Windows 10, version 1903, Windows 10, version 1909, Windows Server version 1903: KB4580386
- Windows 10, version 1809, Windows Server version 1809, Windows Server 2019: KB4580390
- Windows 10, version 1803: KB4586785
- Windows 10, version 1607: KB4586830
- Windows 10, version 1507: KB4586787

Can I save webpages in Internet Explorer mode?

Yes, you can enable the Ctrl+S shortcut for Internet Explorer (IE) mode in Microsoft Edge. To do this, configure the group policy "*Enable extended hot keys in Internet Explorer mode*" located at **Computer Configuration > Administrative Templates > Windows Components > Internet Explorer**.

The ability to use Ctrl+S in IE-Mode requires the following minimum operating system updates:

- Windows 10, version 1809, Windows Server 2019: KB5001342 or later
- Windows 10, version 1909: KB5001337 or later
- Windows 10, version 2004, Windows 10, version 20H2: KB4601319 or later

In addition to the shortcut Ctrl+S, the menuitem **Save page as** in Edge under **Settings and more** (the ellipses icon ...) > **More Tools** can be enabled in Edge 101 (and newer) via the following Group Policy: *Allow Save page as in Internet Explorer mode* located at **Computer Configuration > Administrative Templates > Microsoft Edge**. The ability to use the "Save page as" menuitem requires the following minimum operating system updates:

- Windows 10, version 20H2, Windows 10, version 21H1, Windows 10, version 21H2 : KB5014666 or later
- Windows Server 2022 : KB5014665 or later
- Windows 11 : KB5014668 or later

Can I test a site in Microsoft Edge while it is configured to open IE mode in the Enterprise Mode Site List?

Yes, while you are modernizing your legacy sites, you can test IE mode configured applications on Microsoft Edge. To test these apps, you can configure the InternetExplorerModeTabInEdgeModeAllowed policy. If you enable this policy, your users can open IE mode sites in Microsoft Edge by selecting **Settings and more** (the ellipses icon ...) > **More Tools** > **Open sites in Edge mode**.

How can I debug my legacy application while using IE mode on Microsoft Edge?

You can use IEChooser to launch the Internet Explorer DevTools to debug the content of your IE mode tabs. To use IEChooser, follow these steps:

1. Open IEChooser.
   - Open the Run dialog box. For example, press the `Windows logo key` + `R`.
   - Enter `%systemroot%\system32\f12\IEChooser.exe`, and then select **Ok**.
2. In IEChooser, select the entry for the IE mode tab.

My application requires transferring POST data between IE mode and Microsoft Edge. Is this supported?

Starting with Microsoft Edge Beta channel version 96, navigations that switch between Internet Explorer mode and Microsoft Edge will include form data by default. However, if form data includes file attachments, they will not be transferred between engines. You can choose what data types should be included in such navigations using the InternetExplorerIntegrationComplexNavDataTypes group policy.

In addition to Microsoft Edge version 96, you need to have the following Windows updates installed for this experience:

- Windows 11 KB5007262 or later
- Windows Server 2022 KB5007254 or later
- Windows 10 version 2004; Windows Server version 2004; Windows 10 version; Windows Server version 20H2 and Windows 10 version 21H1 - KB5006738 or later
- Windows 10 version 1909 KB5007189 or later

Where can I find the "Reload in Internet Explorer mode" option?

This feature is available on Microsoft Edge version 92 or later. To enable this option, configure "Allow sites to be reloaded in Internet Explorer mode settings" in Microsoft Edge to "Allow". For more information, see Enable the local site list experience.

Where is the "File > New session" option in Microsoft Edge?

A modern browser solution is available by using multiple profiles in Microsoft Edge. This feature allows you to create a new session with another account. The following resources provide information about the benefits of multiple profiles and how to use them.

- Video: Microsoft Edge and Identity
- Using multiple profiles at work and at home is now easier with Microsoft Edge

Why am I getting multiple authentication prompts when running a page in IE mode on Microsoft Edge?

The client certificate may be requested twice in IE mode. The first time around, the certificate selection dialog will be displayed in IE mode, and the second time around, the dialog will be displayed in Microsoft Edge. Both the frame process and the window process need to request authentication.

After the favicon cache is created, you won't be asked for a client certificate again unless you delete the cache. Alternatively, you can set a rule in your server configuration, such as IIS, not to require a client certificate for the favicon.

Why are there rendering issues like text wrapping and content truncation when child windows are running in IE mode in Microsoft Edge?

The content area of a child window that renders in IE mode in Microsoft Edge is slightly different than what it is on Internet Explorer 11. If a web page has been designed with pixel-based alignments or positioning, you may experience incorrect rendering, text wrapping, and so on.

Two policy settings were added to Microsoft Edge version 95 that let you specify custom adjustments to the height and width of pop-up windows that are generated from IE mode sites via the `window.open` method. You can use the following policies to adjust window size:

- InternetExplorerIntegrationWindowOpenHeightAdjustment - This setting lets you specify a custom adjustment to the height of popup windows generated from the Internet Explorer mode site.
- InternetExplorerIntegrationWindowOpenWidthAdjustment - This setting lets you specify a custom adjustment to the width of popup windows generated from the Internet Explorer mode site.

Why aren't pop-ups or redirected websites loading in IE mode or in Internet Explorer 11?

After configuring IE mode, certain websites, especially those sites that create a new window or a site that gets redirected may not render in IE mode or open in Internet Explorer 11.

For this kind of redirected website, you can make use of the `allow-redirect="true"` in the site list configuration. For more information, see Updated schema elements.

Why aren't websites loading in IE mode when I launch Microsoft Edge for the first time?

Microsoft Edge needs to download the IE mode site list before it can apply IE mode settings. This process may not finish when the browser is starts. A policy is available that can force the loading of the site list before a website is loaded. For more information, see the DelayNavigationsForInitialSiteListDownload policy.

Why can't I open files or pages that are found by using file:// URLs in Microsoft Edge?

For security reasons, Microsoft Edge doesn't allow access to file:// URLs from pages served by HTTP or HTTPS.

If you want this functionality, the following two workarounds are available:

- You can use the IntranetFileLinksEnabled group policy to permit links from HTTPS pages to open Intranet Zone file shares in Windows Explorer.
- Pages loaded from the Intranet Zone into Microsoft Edge's IE mode feature are permitted to navigate directly to URLs using the **file://** protocol.

See also

- Microsoft Edge Enterprise landing page
- About IE mode
- Additional Enterprise Mode information

Microsoft Edge security for your business

11/1/2022 • 4 minutes to read • Edit Online

Microsoft Edge is built on top of the Chromium open source project—the same project that is core to Google Chrome—meaning it shares the same well-engineered and well-tested security architecture and design at its foundation. The Microsoft Edge security story doesn't stop there. In fact, **Microsoft Edge is more secure than Google Chrome for your business on Windows**. It has powerful, built-in defenses against phishing and malware and natively supports hardware isolation on Windows—there's no additional software required to achieve this secure baseline. Furthermore, when paired with native support for Microsoft 365 security and compliance services, Microsoft Edge brings additional, powerful security capabilities and features that help protect against data loss for even more benefits. For more information, watch Video: Microsoft Edge security, compatibility, and manageability.

Let's get into the details, starting with **external threats** and then looking at **internal risks and information protection**.

External threat protection

Highest-rated protection against phishing and malware

Built into Microsoft Edge, Microsoft Defender SmartScreen blocks more phishing and malware attempts than Google Chrome's Safe Browsing, according to an independent test from CyberRatings.org. Microsoft Defender SmartScreen provides real-time reputation checks of sites and downloads as users work online, and is part of the Microsoft Intelligent Security Graph, which draws signals and insights generated from Microsoft's large network of global assets, researchers, and partners. By running checks against dynamic, cloud-based lists of dangerous sites and downloads, Microsoft Edge helps to detect and block even ephemeral threats that quickly disappear.

Microsoft Edge SmartScreen blocked 91.6% of phishing attempts during the "CyberRatings.org Web Browsers vs. Phishing" test and 97.0% of malware attempts during the "CyberRatings.org Web Browsers vs. Malware" test compared to Chrome's Safe Browsing's rates of 89.6% and 88.4%, respectively.

To read the CyberRatings reports:

- go to Browse safer on the web
- click the SmartScreen tab
- select phishing or malware protection to read the reports.

> **NOTE**
> At this time these reports are only available in American English.

The only browser on Windows that natively supports hardware isolation

Microsoft Edge is the only browser on Windows that natively supports hardware isolation capabilities. As part of Windows Pro or Enterprise, Microsoft Defender Application Guard (Application Guard) runs untrusted sites in a kernel isolated from the local device and internal networks. The untrusted sites are run in a "container" so when an attack emerges, it's sandboxed from the rest of the corporate network. For more information, see Microsoft Edge support for Application Guard.

For Chrome, an extension is available to use Windows hardware isolation—the MDAG extension. This extension then launches Microsoft Edge in order to use Application Guard's kernel level isolation. Additionally, to achieve

similar kernel level isolation for a Chrome-only solution, one needs third party isolation software.

> **NOTE**
> Application Guard is available on Windows 10, 1809 and above. Application Guard isn't available on Windows 10 Home editions.

Internal risks and information protection

Native support for Microsoft 365 security without additional software

Aside from protecting against external threats, IT admins also must protect against internal risk. Protecting sensitive corporate data—robustly and at scale—is a top priority for IT administrators, particularly as workforces have decentralized. Microsoft Edge is the only browser withnative support for Azure AD Conditional Access,Windows Information Protection, and the new Microsoft Endpoint Data Loss Prevention (DLP)without additional software required.

Microsoft Edge is the only browser to natively support Conditional Access. Microsoft Edge's support for conditional access makes it easy for organizations to utilize identity signals as part of their access control decisions. Conditional Access is the tool used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. Conditional Access is at the heart of the new identity driven control plane. To get Conditional Access support on Chrome, an additional plug-in is required.

> **NOTE**
> Azure AD Conditional Access requires a Microsoft 365 E3 (or higher) or a Microsoft 365 Business Premium subscription.

Microsoft Edge is the only browser to natively support Windows Information Protection (WIP), which provides protection to corporate data to help prevent accidental leaks by users on Windows devices. Microsoft Edge support for WIP can be configured to only allow IT mandated apps to access corporate data. It also provides leak controls—such as clipboard protection, encrypting files on download, and preventing file uploads to unauthorized network shares or cloud location—with a seamless user experience. WIP works on a perimeter-based configuration, where IT admins define the corporate boundary and all data inside that boundary is considered corporate. Chrome isn't enlightened for WIP with leak controls.

> **NOTE**
> Windows Information Protection (WIP) configuration requires licensing Microsoft Intune or Microsoft Endpoint Configuration Manager, or using a 3rd party mobile device management (MDM) solution, which may have additional licensing requirements.

Microsoft Endpoint data loss prevention (Endpoint DLP) is only supported natively in Microsoft Edge. Endpoint DLP integrates with Microsoft Security Center and extends information protection to Microsoft Edge to help alert users to non-compliant activity and prevent data loss as users work online. It discovers and labels sensitive data inside the enterprise that matches admin-defined criteria, such as files containing credit card numbers or governmental IDs (for example, social security numbers), financial information, etc. Microsoft Information Protection policies can be deployed to Microsoft Endpoint DLP without additional reconfiguration, including sensitive content identifiers and policies that IT admins have already customized. This is seamless deployment of information protection for IT admins.

To learn more about Endpoint DLP prerequisites and how to set up data loss prevention, go to Get started with Endpoint data loss prevention.

NOTE

Microsoft Endpoint data loss prevention requires a Microsoft 365 E5, a Microsoft 365 E5 Compliance, or a Microsoft 365 Business Premium subscription.

See also

- Microsoft Edge Enterprise landing page
- Video: Microsoft Edge security, compatibility, and manageability

Modern security protection for vulnerable legacy apps

11/1/2022 • 6 minutes to read • Edit Online

As the Internet evolved over the last 20 years, so have user needs and expectations for the browsers they use. Today, the Internet is foundational to many businesses, and having a modern browser designed to securely meet business needs is paramount. Microsoft Edge is a modern browser built to securely access the modern web. This article shows how Internet Explorer (IE) mode on Microsoft Edge is more secure than Internet Explorer.

Introduction

Microsoft's internal telemetry shows that the browser is the #1 desktop app. The centrality of the browser as an everyday productivity tool means that the browser presents a large surface area exposed to attacks from the Internet. As the Internet and its applications have become more complex, so have security threats. Over the years, the threat landscape has evolved and attracted sophisticated threat actors including, but not limited to, nation states and organized criminal groups looking to profit via phishing, ransomware, and so on.

Although it's evolved and progressed with iterations up to IE11, IE is still based on technology that's 25 years old. It's a legacy browser that's architecturally outdated and unable to meet the security challenges of the modern web.

To keep an organization's networks safe against today's sophisticated threats, IT admins try to keep users using a modern browser. This ensures that they're protected by modern security features, most or all the time as they browse. Today's common practice of using a modern browser and the IE browser is a convenient workaround, but ineffective. Users who use the IE browser for one activity can easily end up using IE for all activities, which negates the protections that a modern browser provides.

Microsoft Edge is uniquely positioned to provide up-to-date security, enabling users to take advantage modern security technology as much as possible.

Reduce threat surface area

We understand that modernizing your all your legacy sites at once, may not be feasible. With Microsoft Edge and IE mode, you can use a secure modern browser to access your legacy sites before you modernize them. Microsoft Edge with IE mode uses a unique dual-engine system, which lets you open sites with the IE engine or with the new modern engine. The browser engine is determined by the site you visit. Because the older IE engine is less secure, you want to limit use of the legacy engine to only open sites that you trust. Trusted sites are sites you own, control, or know are free of security vulnerabilities. As a best practice you should only access untrusted sites with the modern browser engine because it's more secure.

IE mode is designed to manage access to untrusted site. IE mode uses an "allowlist" where you identify the trusted sites that can use the legacy engine. Any site that's not on the list automatically opens using the modern engine for the safest browsing experience. Untrusted content from untrusted sources is always handled by the modern engine. With IE mode, you control which sites render using the legacy engine, and when you navigate to any other site, Microsoft Edge will automatically switch back to the modern engine. As a result, an organization doesn't have to rely on user behavior and practices to self-regulate and decide which browser to use. From the users' perspective, it's a fluid experience. They don't need to think about what's the 'right' browser to use because Microsoft Edge seamlessly opens the site they're trying to access, whether it's legacy site or a modern site.

IE mode is more secure than IE because toolbars aren't supported, which reduces the surface area for an attack. Toolbars are proven vectors for malware and phishing attacks. Additionally, the IE desktop app will be disabled after retirement, which will eliminate users' time using an outdated browser. Users will be able to access to trusted legacy apps and sites identified in an allowlist for IE mode on Microsoft Edge.

The user will be in a modern environment without needing to adjust their behavior, but also without losing access to mission-critical legacy apps and sites. Microsoft Edge is the only browser that enables users to use a single browser to access both legacy and modern sites.

The next section explains why it's important to minimize the time users spend using the legacy browser engine.

Minimize legacy browser use

The following sections highlight the reasons why it's important to minimize legacy browser engine use.

Architectural deficiency

Architectural deficiency in IE stems from the fact that its original architecture didn't account for the complexity of the modern web or the modern threat landscape. IE evolved from a single process architecture that resulted in inadequate sandboxing and a comparatively broad attack surface. Modern browsers like Microsoft Edge are designed around a threat model based on the current threat landscape. These browsers include security advances like site isolation and hardware-based security features. For example, Intel's Control-flow Enforcement Technology (CET), which handles many modern security threats. These security mitigations are NOT available in IE, making it an easy target for even simple attacks.

Ease of exploitation

IE is easier to exploit than Microsoft Edge because of its architecture and lack of support for modern security features. It's easier to find a single vulnerability in IE that could lead to a Remote Code Execution (RCE) than it is to find a similar weakness in Microsoft Edge, where several vulnerabilities must be chained together to achieve a similar outcome. Additionally, ActiveX and Browser Helper Objects have become vulnerabilities and IE's support for them makes the browser even easier to exploit.

Speed of security patching

Browsers are one of the most used applications on the desktop, used to routinely download, and handle untrusted content from untrusted sources. To stay ahead of security threats, modern browsers can deploy security updates quickly. Because IE is tied to the Windows operating system, the speeds of security updates are limited and causes IE to remain vulnerable for a longer time. In contrast to IE, Microsoft Edge has a built-in updater with a much faster update cadence, reducing response time to days rather than weeks or months.

Security researcher ecosystem

Improving real world browser security relies heavily on a broad ecosystem of external security researchers who are incentivized by bounty programs to find novel vulnerabilities and exploits. Internet Explorer doesn't support a bounty program, which limits the scope of its security improvements. In comparison, Microsoft Edge has a full-fledged bounty program and an internal vulnerability research team to advance state-of-the-art browser security. Because Microsoft Edge is based on Chromium Open Source, it also benefits from Chromium's browser security ecosystem.

Phishing protection using SmartScreen

SmartScreen, Microsoft's phishing protection technology, blocks more phishing [1] and malware [2] attempts than Google Chrome's Safe Browsing, according to an independent study by CyberRatings.org.

> **NOTE**
>
> [1] Web Browsers vs. Phishing, Comparative Test Report (July 2021), CyberRatings.org
>
> [2]Web Browsers vs. Malware, Comparative Test Report (July 2021), CyberRatings.org

Microsoft Edge provides full native support for SmartScreen, but IE is only partially supported because of its outdated architecture.

In addition to providing security advances that map to modern security practices, Microsoft Edge is more secure than Chrome for businesses on Windows 10. Microsoft Edge is also designed to take advantage of the security features, functionality, and tools available in the Microsoft 365 suite and Windows 10. This product ecosystem reduces security and privacy complexity for the IT team. For example, investments and decisions made for identity in Microsoft 365 can be easily applied to Microsoft Edge.

IE mode on Microsoft Edge is a unique solution that ensures users can access mission-critical IE legacy sites, while at the same time staying protected from modern threats.

See also

- About IE mode
- Additional Enterprise Mode information
- Security for your business
- Microsoft Edge Enterprise landing page

Browse more safely with Microsoft Edge

11/1/2022 • 5 minutes to read • Edit Online

This article describes how Microsoft Edge provides enhanced security on the web.

> **NOTE**
> This article applies to Microsoft Edge version 105 or later.

> **IMPORTANT**
> Developers should be aware that the WebAssembly (WASM) interpreter running in enhanced security mode might not yield the expected level of performance. We recommend adding your site as an exception to opt-out of enhanced security mode for site users.

Overview

Microsoft Edge is adding enhanced security protections to provide an extra layer of protection when browsing the web and visiting unfamiliar sites. The web platform is designed to give you a rich browsing experience using powerful technologies like JavaScript. On the other hand, that power can translate to more exposure when you visit a malicious site. With enhanced security mode, Microsoft Edge helps reduce the risk of an attack by automatically applying more conservative security settings on unfamiliar sites and adapts over time as you continue to browse.

Defense in depth

Enhanced security mode in Microsoft Edge mitigates memory-related vulnerabilities by disabling just-in-time (JIT) JavaScript compilation and enabling additional operating system protections for the browser. These protections include Hardware-enforced Stack Protection and Arbitrary Code Guard (ACG).

When combined, these changes help provide 'defense in depth' because they make it more difficult than ever before for a malicious site to use an unpatched vulnerability to write to executable memory and attack an end user. You can learn more about the experimentation results from the Microsoft Edge Security team's blog post and Introducing Enhanced Security for Microsoft Edge.

You may also be interested to learn more about the first line security protections in Microsoft Edge. Notably, you may want to learn more about how Microsoft Edge SmartScreen protects users from phishing scams and malware downloads.

> **NOTE**
> WebAssembly is now supported in enhanced security mode for x64 Windows systems. Additional cross-platform support is expected in the future.

What's new in Microsoft Edge security settings

With **Enhance your security on the web**, Microsoft Edge gives you an extra layer of protection when browsing the web.

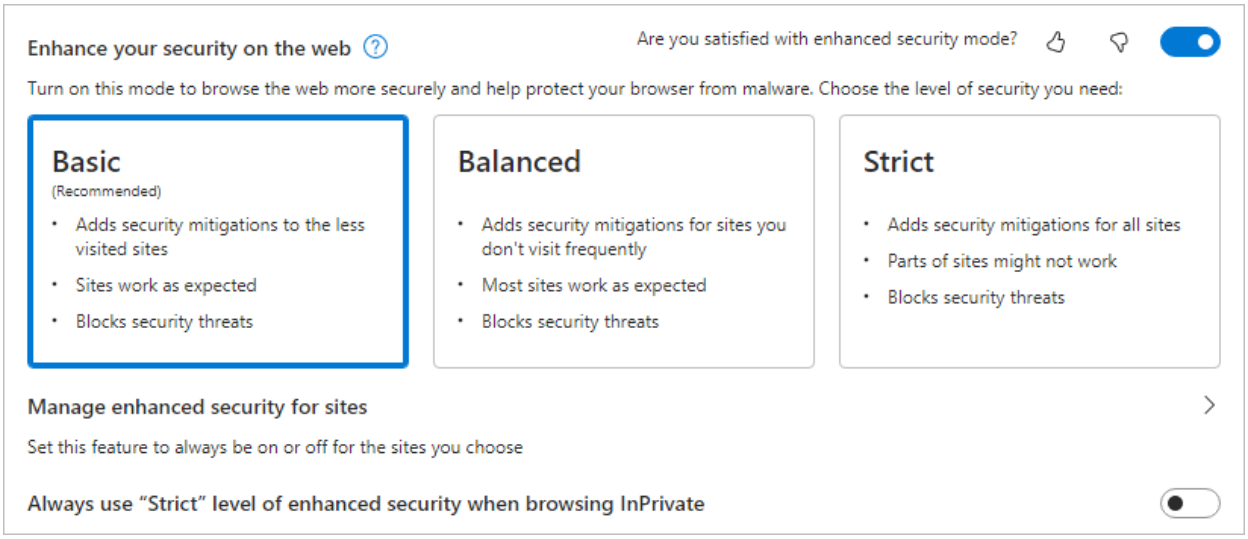
Use the following steps to configure added security.

1. In Microsoft Edge, go to **Settings and more** > **Settings** > **Privacy, search, and services**.
2. Under **Security**, verify that **Enhance your security on the web** is enabled.
3. Select the option that's best for your browsing.

The following toggle settings are available:

- Toggle Off (Default):Feature is turned off
- Toggle On – Basic (Recommended): Microsoft Edge will apply added security protection to the less visited sites. This setting preserves the user experience for the most popular sites on the web.
- Toggle On – Balanced:Microsoft Edge will apply added security protections when users visit unfamiliar sites but bypass those protections for commonly visited sites. This combination provides a practical level of protection against attackers while preserving the user experience for a user's usual tasks on the web.
- Toggle On – Strict: Microsoft Edge will apply added security protections for all the sites a user visits. Users may report some challenges accomplishing their usual tasks.

The following screenshot shows the "Enhance your security on the web" configuration page, with enhanced security mode enabled and set to provide Basic security.


Enhance your security on the web
Are you satisfied with enhanced security mode?
Turn on this mode to browse the web more securely and help protect your browser from malware. Choose the level of security you need:
Basic
(Recommended)
Adds security mitigations to the less visited sites
Sites work as expected
Blocks security threats
Balanced
Adds security mitigations for sites you don't visit frequently
Most sites work as expected
Blocks security threats
Strict
Adds security mitigations for all sites
Parts of sites might not work
Blocks security threats
Manage enhanced security for sites
Set this feature to always be on or off for the sites you choose
Always use "Strict" level of enhanced security when browsing InPrivate

How "Basic" mode works

Basic mode is a static mode that only applies these security mitigations to less visited sites. This mode doesn't take a user's behavior into account and only enables the feature on less visited sites.

How "Balanced" mode works

Balanced mode is an adaptive mode that builds on user's behavior on a particular device, and Microsoft's understanding of risk across the web to give sites that users are most likely to use and trust full access to the web platform, while limiting what new and unfamiliar sites can do.

How "Strict" mode works

As the name suggests, Strict Mode applies these security protections to all sites by default. However, you can still manually add sites to the exception site list and enterprise admin configuration will still apply, if present. Strict mode isn't appropriate for most end users because it may require some level of configuration for the user to complete their normal tasks.

Enhanced security sites

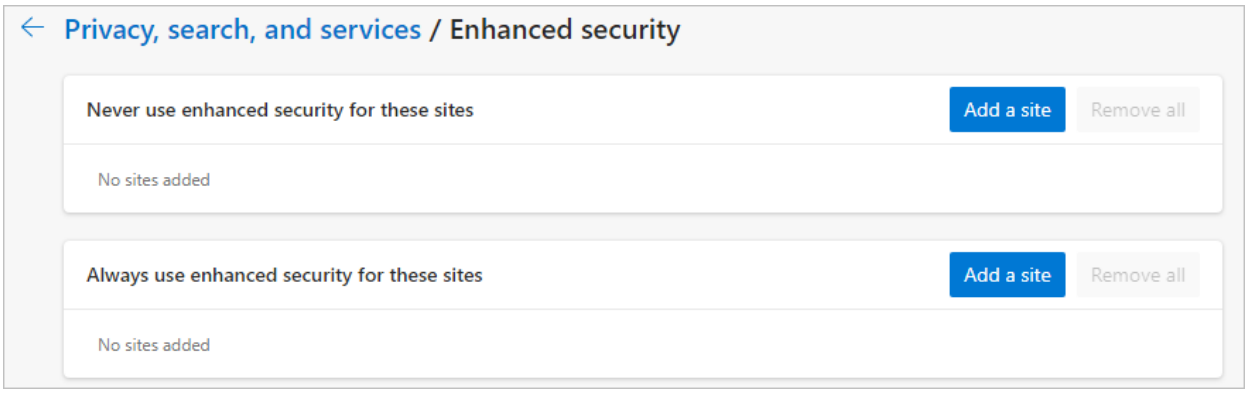
In Basic, Balanced, and Strict mode, you can also create exceptions for certain familiar websites that you trust or wish to enforce this mode on. Use the following steps to add a site to your list.

1. In Microsoft Edge, select **Settings and more** > **Settings** > **Privacy, search, and services**.

2. Verify that **Enhance your security on the web** is turned on.
3. Under **Enhance your security on the web**, select **Manage enhanced security for sites**.
4. Select **Add a site**, type in the full URL, and then select **Add**.

> **NOTE**
> You can use steps (1 - 3) to view sites in **enhanced security sites.**. You can **Edit** a site, **Remove** a site, or **Remove all** exceptions.

The next screenshot shows the settings page for security exceptions.


Privacy, search, and services / Enhanced security
Never use enhanced security for these sites
Add a site
Remove all
No sites added
Always use enhanced security for these sites
Add a site
Remove all
No sites added

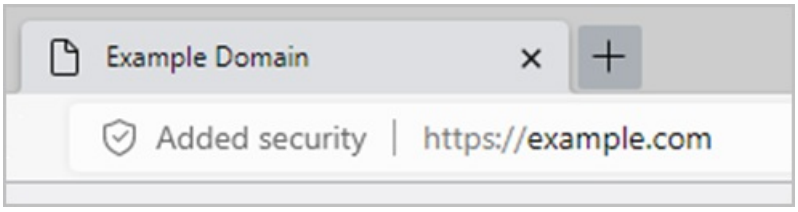
Enterprise controls

Enterprise Admins can configure this security feature using Group Policy settings, including creating "Allow" and "Deny" lists to explicitly enhance security for their users when visiting certain sites, or disable the mode for others. For a complete list of policies, see the Microsoft Edge browser policy documentation.

> **NOTE**
> Setting the EnhanceSecurityMode policy to 'StrictMode' or setting the DefaultJavaScriptJitSetting policy to BlockJavaScriptJit will have the same effect as changing the **Enhance your security on the web** setting in *edge://settings/privacy* to 'Strict'.

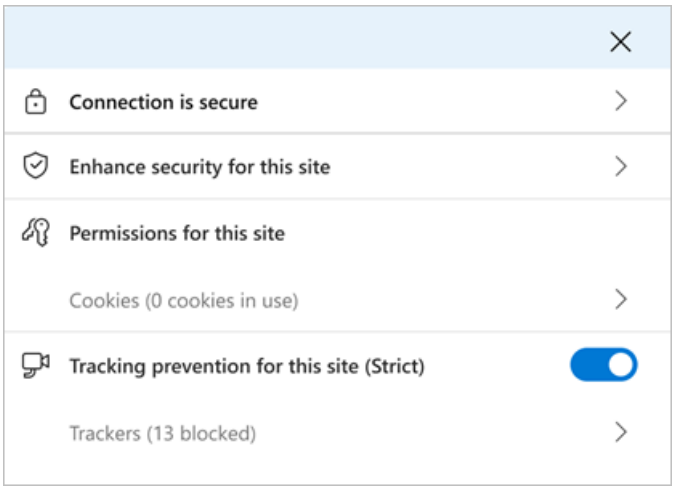
User experience with enhanced security mode

After a user turns on enhanced security mode, they'll see a banner with the words "Added security" in their URL navigation bar when Microsoft Edge is applying enhanced security mode for a particular site.



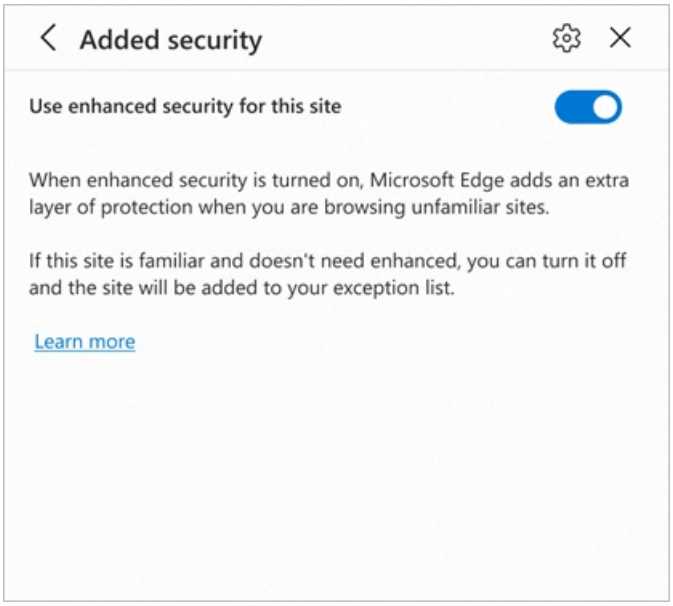
When you select the banner, you'll see the next flyout. You can select "Enhance security for this site" to redirect you to a second flyout that shows the security settings for the current site and gives the user the option to toggle security on or off.

> **NOTE**
> "Enhance security for this site" only appears when enhanced security mode is enabled in Microsoft Edge Settings.


Connection is secure
Enhance security for this site
Permissions for this site
Cookies (0 cookies in use)
Tracking prevention for this site (Strict)
Trackers (13 blocked)

In the flyout shown in the next screenshot, you can manually enable or disable enhanced security mode for a particular site. If you change the "Use enhanced security for this site" toggle, Microsoft Edge will proactively add that site to the exception site list.

> **NOTE**
> You can always remove this site by updating the exception site list in **Settings** > **Privacy, search, and services** > **Enhanced security exceptions**.


Added security
Use enhanced security for this site
When enhanced security is turned on, Microsoft Edge adds an extra layer of protection when you are browsing unfamiliar sites.
If this site is familiar and doesn't need enhanced, you can turn it off and the site will be added to your exception list.
Learn more

Send us feedback

We want to get your feedback on our next iteration to improve "enhanced security mode". If something doesn't work the way you expect, or if you have feedback to share on these changes, we want to hear from you. You can reach out to Microsoft Support to report issues or feedback. You can also leave feedback in our TechCommunity forum.

See also

- Video: Secure browsing on Microsoft Edge
- Super Duper Secure Mode
- Microsoft Edge Enterprise landing page

Identify and interrupt downloads of potentially dangerous files

11/1/2022 • 3 minutes to read • Edit Online

Microsoft Edge's File Type Policies component classifies files by their level of "dangerousness" to manage file downloads. A harmless file (for example, a `.txt` file) can be downloaded freely, while a potentially dangerous file like a `.dll` is subjected to a higher degree of vetting. This scrutiny provides a more security-conscious user experience.

How Microsoft Edge determines the danger level of a file type

Microsoft Edge inherits its file type policies from the upstream Chromium browser. You can view these file types and their classification in the download_file_types.asciipb file. In this file, you'll see that each type has a **danger_level**, which is one of three values: `DANGEROUS`, `NOT_DANGEROUS`, or `ALLOW_ON_USER_GESTURE`.

The following two classifications are simple:

- **NOT_DANGEROUS** means that the file is safe to download, even if the download request was accidental.
- **DANGEROUS** means that the browser should always warn the user that the download may harm their device.

The third setting, **ALLOW_ON_USER_GESTURE** is more subtle. These files are potentially dangerous, but most likely harmless if the user requests the download. Microsoft Edge will allow these downloads to continue automatically if **two** conditions are **both** met:

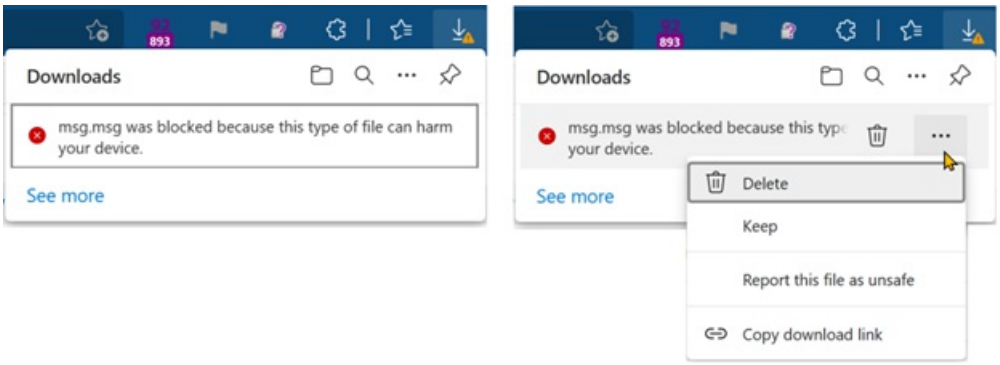
- There's a user gesture associated with the network request that started the download. For example, the user clicked a link to the download.
- There's a recorded prior visit to the referring origin (the page that links to the download) before the most recent midnight (that is, yesterday or earlier). This recorded visit implies that the user has a history of visiting the site.

The download will also continue automatically if the user explicitly starts it by using the **Save link as** context menu command, enters the download's URL directly into the browser's address bar, or if Microsoft Defender SmartScreen indicates that the file is safe.

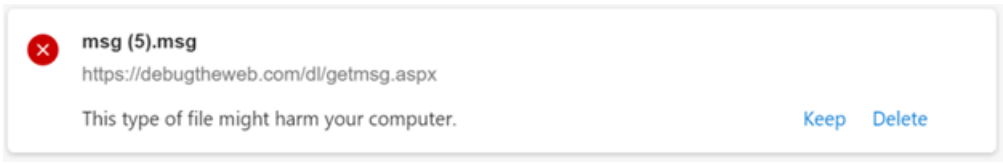
> **NOTE**
> Starting in version 91, Microsoft Edge will interrupt downloads that lack the required gesture.

User experience for downloads that lack a gesture

If a download for a potentially dangerous type starts without the required gesture, Microsoft Edge states that the download "was blocked". Commands named `Keep` and `Delete` are available from the ... (ellipsis) option on the download item to let the user continue or cancel the download.



On the `edge://downloads` page, the user will see the same options. The next screenshot shows and example of these options.



Enterprise controls for downloads

While users are unlikely to encounter download interruptions for sites they use every day, they might encounter them for legitimate downloads on sites that they use rarely. To help streamline the user-experience for Enterprises, a Group Policy is available.

Enterprises can use ExemptDomainFileTypePairsFromFileTypeDownloadWarnings to specify the filetypes that are allowed to download from specific sites without interruption. For example, the following policy lets XML files download from contoso.com and woodgrovebank.com without interruption, and MSG files download from any site.

```
[{"file_extension":"xml","domains":["contoso.com", "woodgrovebank.com"]}, {"file_extension":"msg", "domains":["*"]}]
```

File types requiring a gesture

The latest file types policies are published in the Chromium source code. As of May 2021, file types with a `danger_level` of `ALLOW_ON_USER_GESTURE` on at least one OS platform include:

```
crx, pl, py, pyc, pyo, pyw, rb, efi, oxt, msi, msp, mst, ade, adp, mad, maf, mag, mam, maq, mar, mas, mat,
mav, maw, mda, mdb, mde, mdt, mdw, mdz, accdb, accde, accdr, accda, ocx, ops, paf, pcd, pif, plg, prf, prg,
pst, cpi, partial, xrm-ms, rels, svg, xml, xsl, xsd, ps1, ps1xml, ps2, ps2xml, psc1, psc2, js, jse, vb, vbe,
vbs, vbscript, ws, wsc, wsf, wsh, msh, msh1, msh2, mshxml, msh1xml, msh2xml, ad, app, application, appref-ms,
asp, asx, bas, bat, chi, chm, cmd, com, cpl, crt, cer, der, eml, exe, fon, fxp, hlp, htt, inf, ins, inx, isu,
isp, job, lnk, mau, mht, mhtml, mmc, msc, msg, reg, rgs, scr, sct, search-ms, settingcontent-ms, shb, shs,
slk, u3p, vdx, vsx, vtx, vsdx, vssx, vstx, vsdm, vssm, vstm, vsd, vsmacros, vss, vst, vsw, xnk, cdr, dart,
dc42, diskcopy42, dmg, dmgpart, dvdr, dylib, img, imgpart, ndif, service, smi, sparsebundle, sparseimage,
toast, udif, action, definition, wflow, caction, as, cpgz, command, mpkg, pax, workflow, xip, mobileconfig,
configprofile, internetconnect, networkconnect, pkg, deb, pet, pup, rpm, slp, out, run, bash, csh, ksh, sh,
shar, tcsh, desktop, dex,apk
```

The file type danger level may vary by operating system

File type settings sometimes vary depending on the client OS platform. For instance, an `.exe` file isn't dangerous on a Mac, while an `.applescript` file is harmless on Windows.

Allow list for Microsoft Edge endpoints

11/1/2022 • 2 minutes to read • Edit Online

Microsoft Edge requires connectivity to the Internet to support its features. This article identifies the domain URLs that you need to add to the Allow list to ensure communications through firewalls and other security mechanisms.

> **NOTE**
> This applies to Microsoft Edge version 77 or later.

Domain URLs to allow

Allow the following domain URLs for Microsoft Edge.

Update Service

The service that Microsoft Edge uses to check for new updates.

- `https://msedge.api.cdp.microsoft.com`

Experimentation and Configuration service

- `https://config.edge.skype.com`

Download locations for Microsoft Edge

Locations Microsoft Edge can be downloaded from during an initial install or when an update is available. The download location is determined by the Update Service.

HTTP

- `http://msedge.f.tlu.dl.delivery.mp.microsoft.com`
- `http://msedge.f.dl.delivery.mp.microsoft.com`
- `http://msedge.b.tlu.dl.delivery.mp.microsoft.com`
- `http://msedge.b.dl.delivery.mp.microsoft.com`

HTTPS

- `https://msedge.sf.tlu.dl.delivery.mp.microsoft.com`
- `https://msedge.sf.dl.delivery.mp.microsoft.com`
- `https://msedge.sb.tlu.dl.delivery.mp.microsoft.com`
- `https://msedge.sb.dl.delivery.mp.microsoft.com`

> **TIP**
> To simplify the allow list for download locations a wild card can be used: `*.dl.delivery.mp.microsoft.com`

Download locations for Microsoft Edge Extensions

Locations Microsoft Edge Extensions can be downloaded from during an initial install or when an update is available. The download location is determined by the Update Service.

HTTP

- `http://msedgeextensions.f.tlu.dl.delivery.mp.microsoft.com`
- `http://msedgeextensions.f.dl.delivery.mp.microsoft.com`
- `http://msedgeextensions.b.tlu.dl.delivery.mp.microsoft.com`
- `http://msedgeextensions.b.dl.delivery.mp.microsoft.com`

HTTPS

- `https://msedgeextensions.sf.tlu.dl.delivery.mp.microsoft.com`
- `https://msedgeextensions.sf.dl.delivery.mp.microsoft.com`
- `https://msedgeextensions.sb.tlu.dl.delivery.mp.microsoft.com`
- `https://msedgeextensions.sb.dl.delivery.mp.microsoft.com`

> **TIP**
> To simplify the allow list for download locations a wild card can be used: `*.dl.delivery.mp.microsoft.com`

Optionally for Download Delivery Optimization

For information about delivery optimization, see Delivery Optimization for Windows 10 updates.

- Client to Service communication: `*.do.dsp.mp.microsoft.com` (HTTP Port 80, HTTPS Port 443)
- Client to Client communication: TCP port 7680 should be open for inbound traffic

Sync

These endpoints manage the reading and writing of synced data, rights management for secure data, and notifying the browser when new sync data is available.

- Microsoft Edge sync service endpoints:
  - `https://edge-enterprise.activity.windows.com`
  - `https://edge.activity.windows.com`
- Azure Information Protection endpoints:
  - `https://api.aadrm.com` (for most tenants)
  - `https://api.aadrm.de` (for tenants in Germany)
  - `https://api.aadrm.cn` (for tenants in China)
- Windows Notification Service endpoints

Cloud Site List Management

The service that Microsoft Edge uses to download the cloud-hosted site list for Internet Explorer (IE) mode. For more information, see Cloud Site List Management

- `https://edge.microsoft.com/`

Other browser support services

Provide metadata for browser features such as tracking protection, certificate revocation lists, and other browser component updates. Provide downloadable spellcheck dictionaries and ad-blocking block lists. Provide services to support browser features such as collections, autofill, and extension store.

- `http://edge.microsoft.com/`
- `https://edge.microsoft.com/`

See also

- Microsoft Edge Enterprise landing page
- Microsoft Edge documentation landing page
- Manage connection endpoints for Windows 10 Enterprise, version 1903

Understand Data Loss Prevention (DLP) in Microsoft Edge

11/1/2022 • 2 minutes to read • Edit Online

This article describes how Microsoft Edge supports data loss prevention (DLP) with Endpoint DLP and Windows Information Protection (WIP).

DLP defined

Data loss prevention (DLP) is a system of technologies that identify and safeguard sensitive enterprise data from unauthorized disclosure. To comply with business standards and industry regulations, organizations must protect sensitive information and prevent its unauthorized disclosure. Sensitive information includes financial data or personal information. Some examples of personal information include credit card numbers, social security numbers, and health records.

Remote work has increased the emphasis on using DLP. With the growing use of personal and work activities on devices, enterprises are seeing an increased risk of unauthorized sharing of corporate data outside the workplace.

This blending of user activities has also spread to devices, where data is moved between personal and corporate devices over various public and private networks. The net result is a dramatically increased risk of exposing sensitive data.

Microsoft Edge natively supports two different DLP solutions, Microsoft Endpoint DLP and Windows Information Protection (WIP).

Microsoft Endpoint data loss prevention (Endpoint DLP)

Microsoft Endpoint DLP is the next generation of data loss prevention using modern concepts such as data-centric protection. It's built-in to Windows 10 and Microsoft Edge so it doesn't need more agents or plugins on the device.

> **NOTE**
> This applies to Microsoft Edge version 85 or later.

To learn more about Endpoint DLP, use the following resources:

- Video: Microsoft Edge and Data loss prevention (DLP)
- Learn about Microsoft 365 Endpoint data loss prevention
- Get started with Endpoint data loss prevention

Microsoft Edge enforces admin-configured policies for sensitive files, and records audit events for non-compliant activities.

Some of the user activities that you can audit and manage on devices running Windows 10 include the following activities:

- File Upload: Protect sensitive file upload to unauthorized cloud locations.
- Clipboard Protection: Protect sensitive data from being copied out of the file.

- Print Protection: Protect sensitive file from being printed.
- Save to USB/Network: Protect sensitive file from being saved to removable USB storage or unauthorized network locations.

For more detailed information about user activities you can audit and manage, see Endpoint activities you can monitor and take action on.

Windows Information Protection

> **NOTE**
> Windows information protection will be discontinued over time. For more information, see Announcing the sunset of Windows Information Protection (WIP).

Check out Support for Windows Information Protection, which describes how Microsoft Edge supports Windows Information Protection (WIP). You can learn moe about system requirements, benefits, and supported features in the following sections:

- System Requirements
- Windows Information Protection Benefits
- WIP features supported in Microsoft Edge

See also

- Microsoft Edge Enterprise landing page
- Video: Data loss prevention - Microsoft Edge
- Overview of data loss prevention
- Protect your enterprise data using Windows Information Protection

Password Monitor auto-enabled for users

11/1/2022 • 3 minutes to read • Edit Online

This article describes how Password Monitor in Microsoft Edge will be turned on for select users and gives admins the steps to control how monitoring is enabled.

> **NOTE**
> This article applies to Microsoft Edge version 88 or later.

Introduction, benefits, and availability

Password Monitor helps Microsoft Edge users protect their online accounts by informing them if any of their passwords have been found in an online leak. Online leaks or data breaches happen when bad actors steal data from third-party apps or websites. To learn more, see the Password Monitor: Safeguarding passwords in Microsoft Edge paper on the Microsoft Research Blog.

Benefits

Given the frequency and scope of these online attacks having this kind of protection has become necessary for everyone. Microsoft Edge has the built-in ability to securely check a user's saved passwords against passwords that are known to be compromised and alerts them if a match is found.

Configure group policy for Password Monitor

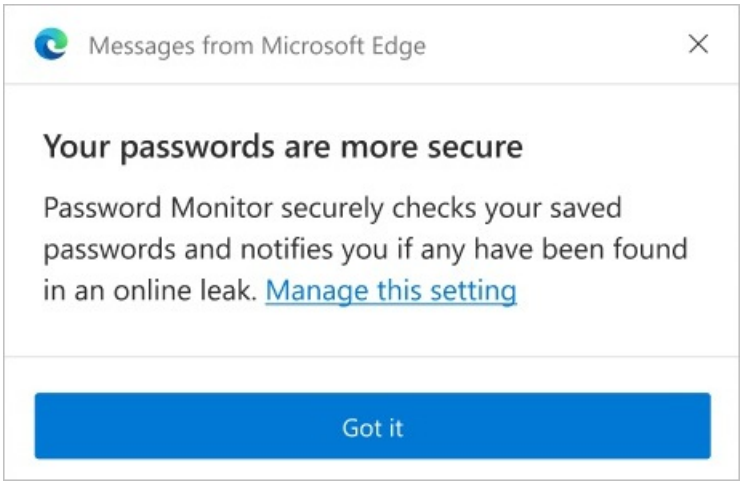
This feature is controlled via the PasswordMonitorAllowed group policy.

After the policy is enabled, users still need to provide consent to turn on the feature. Consent is required because the feature contains user's sensitive and personal data (passwords). If the feature is disabled using group policy, users can't override this setting.

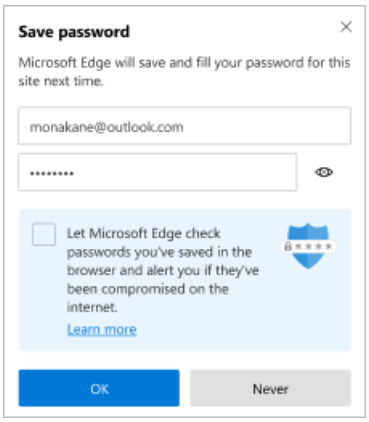
Enabling Password Monitor for users

After the password monitor policy is enabled, there are different ways this feature is made available to users.

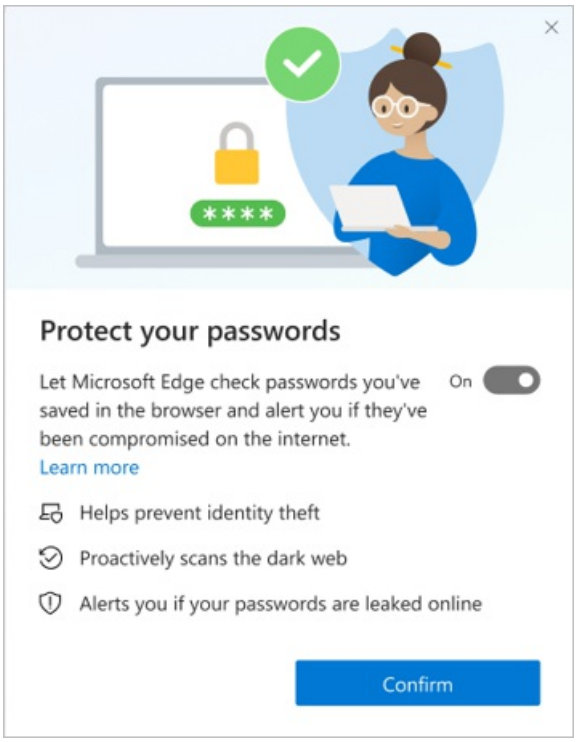
- Auto-enablement. Users that are signed-in using their work account (Active Directory or Azure Active Directory) and syncing their passwords will be auto-enabled for this feature. They will see the notification in the next screenshot informing them that the feature's turned on.


Messages from Microsoft Edge
Your passwords are more secure
Password Monitor securely checks your saved passwords and notifies you if any have been found in an online leak. Manage this setting
Got it

- Getting explicit consent. Users that don't have Password Sync turned on will be asked for permission to turn on Password Monitor. They will be prompted when the following actions happen:
    - When a user is saving a new password.


Save password
Microsoft Edge will save and fill your password for this site next time.
monakane@outlook.com
Let Microsoft Edge check passwords you've saved in the browser and alert you if they've been compromised on the internet.
Learn more
OK
Never

    - When a user has signed-in to the browser using a saved password.


Protect your passwords
Let Microsoft Edge check passwords you've saved in the browser and alert you if they've been compromised on the internet.
On
Learn more
Helps prevent identity theft
Proactively scans the dark web
Alerts you if your passwords are leaked online
Confirm

- Direct activation. Users can go to **Settings** > **Passwords** anytime and turn the feature On or Off.

User scenarios with Password Monitor auto-enabled

The following table shows scenarios where Password Monitor is auto-enabled and how it will work on user devices.

SCENARIO	BASE CONDITIONS	IMPACT
1 with Sync on	Sync ON Feature enabled previously: No Response to Consent UI: None	Feature enabled by default and a notice bubble is shown 2 min after browser starts. - If sync is turned off after that, the feature is disabled. - Feature turned off before altering sync, sync will no longer affect the feature.

SCENARIO	BASE CONDITIONS	IMPACT
2 with Sync on	Sync ON Feature enabled previously: Yes Response to Consent UI: None	Feature stays the same as user choice. Notice bubble isn't shown and there's no affect of sync change on feature value.
3 with Sync off	Sync Off Feature enabled previously: No Response to Consent UI: None	Sync will be off and the feature will stay disabled - At any point after that if user turns the sync on without altering the feature: the feature is enabled and auto-enablement notification is shown 2 minutes after Sync is turned on. - If sync is turned off again, the feature is disabled - If the feature is changed before turning on sync, sync will no longer affect Password Monitor.
4 with Sync off	Sync OFF Feature enabled previously: Yes Response to Consent UI: None	Feature stays the same as user choice, notice bubble isn't shown, and there's no effect of sync change on the feature value.

In addition, if a user is signed-in using a work account that is restricted via policies for any of the following, the feature will NOT be auto-enabled for them:

- Password Monitor is disabled
- Password Sync is disabled
- Sharing of data with Microsoft servers is disabled

Frequently Asked Questions

How can Password Monitor be disabled for my organization?

You can disable Password Monitor for your organization by:

- Using the PasswordMonitorAllowed group policy.
- Stopping data from being synchronized and sent to Microsoft servers.

> **NOTE**
> Password Monitor can work even if Password Sync is disabled, as long as the user has given explicit consent to turn the feature On or have turned it on themselves via Settings.

What happens if a user for whom the feature has been auto-enabled, turns Password Monitor off via Settings?

The user setting is honored and the feature will remain disabled for that user. However, they might be shown a consent dialog again in case they've never previously responded to the consent prompt.

See also

- Microsoft Edge Enterprise landing page

Microsoft Edge password manager security

11/1/2022 • 9 minutes to read • Edit Online

The frequently asked questions in this article describe how Microsoft Edge's built-in password manager provides security for user passwords.

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

How are passwords stored in Microsoft Edge and how safe is this approach?

Microsoft Edge stores passwords encrypted on disk. They're encrypted usingAES and the encryption key is saved in an operating system (OS) storage area. This technique is calledlocal data encryption. Although not all of the browser's data is encrypted, sensitive data such as passwords, credit card numbers, and cookies are encrypted when they are saved.

The Microsoft Edge password manager encrypts passwords so they can only be accessed when a user is logged on to the operating system. Even if an attacker has admin rights or offline access and can get to the locally stored data, the system is designed to prevent the attacker from getting the plaintext passwords of a user who isn't logged in.

The way to decrypt another user's passwords is if that user were logged on and the attacker had the user's password or has compromised the domain controller.

About the encryption method

Theprofile's encryption keyis protected usingChromium's OSCrypt and uses the following platform-specific OS storage locations:

- On Windows, the storage area is DPAPI
- On Mac, the storage area is the Keychain
- On Linux, the storage area is Gnome Keyring or KWallet

All these storage areas encrypt the AES key using a key accessible to some or all processes running as the user. This attack vector is often featured in blogs as a possible 'exploit' or 'vulnerability', which is an incorrect understanding of the browser threat model and security posture.

However, physically local attacks and malware are outside the threat model and, under these conditions, encrypted data would be vulnerable. If your computer's infected with malware, an attacker can get decrypted access to the browser's storage areas. The attacker's code, running as your user account, can do anything you can do.

Why encrypt data locally? Why not store the encryption key elsewhere, or make it harder to obtain?

Internet browsers (including Microsoft Edge) aren't equipped with defenses to protect against threats where the entire device is compromised due to malware running as the user on the computer. However, programs like Microsoft Defender SmartScreen and OS-level protections like Windows Defender are designed to ensure that

the device isn't compromised to start with.

Despite its inability to protect against full-trust malware, Local Data Encryption is useful in certain scenarios. For example, if an attacker finds a way to steal files from the disk without the ability to execute code or has stolen a laptop that isn't protected with Full Disk Encryption, Local Data Encryption will make it harder for the thief to get the stored data.

Do you recommend storing passwords in Microsoft Edge?

Users who can rely on the Microsoft Edge's in-built password manager can (and do) use stronger and unique passwords more because they don't need to remember them all and type them as often. And because the password manager will only autofill passwords on the sites to which they belong, users are less likely to fall for a phishing attack.

> **NOTE**
> Industry reports show that 80% of online incidents are related to phishing, and more than 37% of untrained users fail phishing tests.

Microsoft Edge's password manager is convenient and easily distributed, which contributes to improved security. When combined with sync, you can get all your passwords on all your devices and it's easy to use a different password for every website. You can use long and complex passwords that you don't have to remember for every site and skip the hassle of typing a complex string every single time. Password manager's convenience means there's less risk of falling for a phishing attack.

However, using a password manager that's keyed to the user's operating system login session also means that an attacker in that session can immediately retrieve all the user's saved passwords. Without a password manager to steal from, an adversary would need to track keystrokes or monitor submitted passwords.

The decision of whether to use a password manager comes down to assessing the many benefits we've described against the possibility of the entire device getting compromised. For most threat models, using the Microsoft Edge password manager is the recommended option.

> **NOTE**
> If an enterprise is concerned about theft of a specific password or a site getting compromised because of a stolen password, additional precautions should be taken. Some effective solutions that help mitigate this kind of incident is Single Sign On (SSO) via Active Directory, Azure Active Directory, or a third party. Other solutions include 2FA (such as MS Authenticator) orWebAuthN.

Should a password manager be enabled by an organization?

The simple and easy answer is: Yes, use the browser's password manager.

A more complete response means having in-depth knowledge of your threat model because security options and choices vary depending on different threat models. Some relevant questions to consider when thinking about whether you should enable the password manager for your organization are:

- What kind of attackers are you worried about?
- What kind of websites do your users log on to?
- Do your users select strong, unique passwords?
- Are your users' accounts protected with 2FA?

- What kind of attacks are most likely?
- How do you protect your enterprise devices from malware?
- What's your users' personal tolerance for inconvenience?
- Consider the impact of data sync.

It's important to factor in the security of user data as it gets synced to various user devices and the amount of control the organization has on autofill data syncing.

Data syncing and Microsoft Edge:

- Data syncing can be enabled or disabled as desired across the organization.
- Data security in transit and at rest in the cloud: All synced data is encrypted in transit over HTTPS when transferred between the browser and Microsoft servers. The synced data is also stored in an encrypted state on Microsoft servers. Sensitive data types such as addresses, and passwords are further encrypted on the device before being synced. If you're using a work or school account, all data types are further encrypted before being synced using Microsoft Purview Information Protection.

Why do Microsoft security baselines recommend disabling the password manager?

The Microsoft security team has currently rated the impact of a worm that compromises a network of Enterprise PCS (resulting in loss of all credentials in all devices' password managers) as more severe than the (more likely but lower impact) risk of targeted phishing attacks that compromise a single user-entered credential.

This assessment is under discussion and subject to change with the addition of new security-enhancing features in Microsoft Edge.

Can malicious extensions gain access to passwords?

An extension with permission to interact with a page is inherently able to access anything from that page, including an auto filled password. Similarly, a malicious extension can modify the contents of form fields and network requests/responses to misuse the authority of the current user login context.

However, Microsoft Edge provides an extensive set of policies that enable fine control over installed extensions. Using the policies in the following table is necessary to protect corporate data.

POLICY	CAPTION
BlockExternalExtensions	Blocks external extensions from being installed
ExtensionAllowedTypes	Configure allowed extension types
ExtensionInstallAllowlist	Allow specific extensions to be installed
ExtensionInstallBlocklist	Control which extensions cannot be installed
ExtensionInstallForcelist	Control which extensions are installed silently
ExtensionInstallSources	Configure extension and user script install sources
ExtensionSettings	Configure extension management settings

How does the Microsoft Edge password manager compare with a third-party product?

The following table shows how Microsoft Edge password manager compares to third-party password managers.

THIRD-PARTY PASSWORD MANAGER	MICROSOFT EDGE PASSWORD MANAGER
Server sync. Some products store passwords in the cloud to sync all your devices. This feature is helpful, but there's a risk if the cloud service gets compromised and your data is exposed. **Remarks:** The risk is mitigated by having passwords encrypted in the cloud and storing the encryption key on your device(s) so attackers can't get to the key and your passwords.	There's a cloud exposure risk because passwords are synced across Windows devices that have Microsoft Edge installed. **Remarks:** This risk is mitigated by the data security steps covered in this article.
Trust. It's necessary to trust that the third party isn't doing anything malicious, such as sending your passwords to another party. **Remarks:** This risk can be mitigated by reviewing the source code (in the case of open-source products), or by believing that the vendor cares about their reputation and revenue.	**Remarks:** Microsoft is a known and trusted vendor with decades of history in providing enterprise-grade security and productivity, with resources designed to protect your passwords worldwide.
Supply chain security. It's hard to verify that the vendor has secure supply chain/build/release processes for the source code.	**Remarks:** Microsoft has robust internal processes to ensure minimal risk to source code.
Compromised client or account. If a client device or user account is compromised, an attacker can get the passwords. **Remarks:** This risk is mitigated for some password managers that require the user to enter a Master Password that's not stored locally to decrypt the passwords. A Master Password is only partial mitigation because an attacker could read keystrokes and get the master password as it's typed or read passwords from process memory when filling in a form field.	**Remarks:** Microsoft offers OS-level protections like Windows Defender, designed to ensure that the device isn't compromised to start with. However, if a client device is compromised, an attacker may be able to decrypt the passwords.

> **NOTE**
>
> Third-party products might provide protection against additional threat models, but this is at the expense of complexity or ease-of-use. The Microsoft Edge password manager is designed to provide convenient and easy-to-use password management that can be fully controlled by IT Admins using Group Policy and doesn't require trusting a third party.

Why doesn't Microsoft offer a Master Password to protect the data?

When browser passwords are encrypted on disk, the encryption key is available to any process on your device, which includes anylocally running malware. Even if passwords are encrypted in a "vault" by a master key, they'll be decrypted when loaded in the browser's memory space and can be harvested after you unlock the vault.

A Master Password feature (that authenticates the user before auto-filling their data) provides a trade-off in convenience for broader threat mitigation. Specifically, it helps to reduce the window of data exposure against latent malware or physically local attackers. However, a Master Password is not a panacea, and local attackers and dedicated malware have various strategies for circumventing the protection of a Master Password.

NOTE

Microsoft Edge now offers the ability to enable authentication before autofill capability; this provides users an additional layer of privacy and prevents their stored passwords from being used by anyone but them. For more details, see Additional privacy for your saved passwords.

Can using a password manager impact my privacy?

No, not if steps are taken to protect access to your saved passwords.

There's a known exploit that some advertisers use, which uses stored passwords to uniquely identify and track users. For more information, seeAd targeters are pulling data from your browser's password manager. Browsers have taken steps to mitigate thisprivacy issue.The PasswordValueGatekeeper class can be used to limit access to the password field data, even when the browser is configured to autofill when it loads.

This user information harvesting threat can be easily mitigated by enabling the optional edge://flags/#fill-on-account-selectfeature. This feature only allows passwords to be added to a form field after the user explicitly chooses a credential, which ensures that users stay aware of who is receiving their passwords.

See also

Microsoft Edge Enterprise landing page

How Microsoft Edge is more secure than Chrome for business on Windows 10

Protect against potentially unwanted applications (PUAs)

11/1/2022 • 3 minutes to read • Edit Online

This article explains how you can protect against potentially unwanted applications (PUAs) using Microsoft Edge or by using Windows Defender Antivirus.

> **NOTE**
> This article applies to Microsoft Edge version 80 or later.

Overview

Potentially unwanted applications aren't considered to be viruses or malware, but these apps might perform actions on endpoints that adversely affect endpoint performance or use. For example, *Evasion software* actively tries to evade detection by security products. This kind of software can increase the risk of your network being infected with actual malware. PUA can also refer to applications that are considered to have poor reputation.

For a description of the criteria used to classify software as a PUA, see Potentially unwanted application.

Protect against PUA with Microsoft Edge

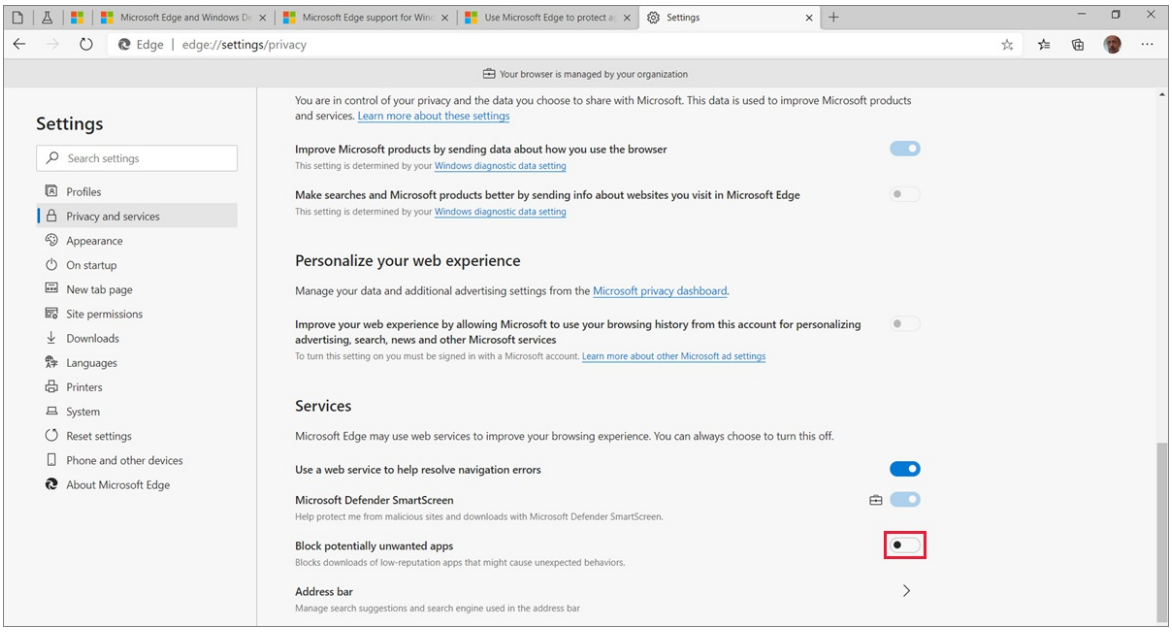
Microsoft Edge (version 80.0.361.50 or later) blocks PUA downloads and associated resource URLs.

You can set up protection by enabling the **Block potentially unwanted apps** feature in Microsoft Edge.

> **NOTE**
> The Microsoft Edge Team blog post describes this new feature and explains how to handle a mislabeled app or report an app as unwanted.

To enable PUA protection:

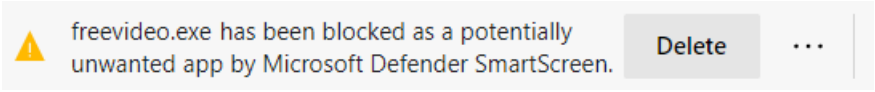
1. Open **Settings** in the browser.
2. Select **Privacy and services**.
3. In the **Services** section, check to see that **Microsoft Defender SmartScreen** is turned on. If not, then turn on Microsoft Defender SmartScreen. The example in the following screenshot shows the browser is managed by the organization and that Microsoft Defender SmartScreen is turned on.


Settings
Search settings
Profiles
Privacy and services
Appearance
On startup
New tab page
Site permissions
Downloads
Languages
Printers
System
Reset settings
Phone and other devices
About Microsoft Edge
Your browser is managed by your organization
You are in control of your privacy and the data you choose to share with Microsoft. This data is used to improve Microsoft products and services. Learn more about these settings
Improve Microsoft products by sending data about how you use the browser
This setting is determined by your Windows diagnostic data setting
Make searches and Microsoft products better by sending info about websites you visit in Microsoft Edge
This setting is determined by your Windows diagnostic data setting
Personalize your web experience
Manage your data and additional advertising settings from the Microsoft privacy dashboard.
Improve your web experience by allowing Microsoft to use your browsing history from this account for personalizing advertising, search, news and other Microsoft services
To turn this setting on you must be signed in with a Microsoft account. Learn more about other Microsoft ad settings
Services
Microsoft Edge may use web services to improve your browsing experience. You can always choose to turn this off.
Use a web service to help resolve navigation errors
Microsoft Defender SmartScreen
Help protect me from malicious sites and downloads with Microsoft Defender SmartScreen.
Block potentially unwanted apps
Blocks downloads of low-reputation apps that might cause unexpected behaviors.
Address bar
Manage search suggestions and search engine used in the address bar

4. In the **Services** section, use the toggle shown in the preceding screenshot to turn on **Block potentially unwanted apps**.

> **TIP**
>
> You can safely explore the URL-blocking feature of PUA protection by testing it out on one of our Windows Defender SmartScreen demo pages.

When Microsoft Edge detects a PUA, you will see a message like the one in the next screenshot.



To block against PUA-associated URLs

After you turn on PUA protection in Microsoft Edge, Windows Defender SmartScreen will protect you from PUA-associated URLs.

There are several ways admins can configure how Microsoft Edge and Windows Defender SmartScreen work together to protect users from PUA-associated URLs. For more information, see:

- Configure Microsoft Edge policy settings on Windows
- SmartScreen settings
- SmartScreenPuaEnabled policy
- Configure Windows Defender SmartScreen

Admins can also customize the Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) block list. They can use the Microsoft Defender ATP portal to create and manage indicators for IPs and URLs.

Protect against PUA with Windows Defender Antivirus

The Detect and block potentially unwanted applications article also describes how you can configure Windows Defender Antivirus to enable PUA protection. You can configure protection using any of the following options:

- Microsoft Intune
- Microsoft Endpoint Configuration Manager
- Group Policy
- PowerShell cmdlets

When Windows Defender detects a PUA file on an endpoint it quarantines the file and notifies the user (unless notifications are disabled) in the same format as a normal threat detection (prefaced with "PUA:".) Detected threats also appear in the quarantine list in the Windows Security app.

PUA notifications and events

There are several ways an admin can see PUA events:

- In the Windows Event Viewer, but not in Microsoft Endpoint Configuration Manager or Intune.
- In an email if email notifications for PUA detections is turned on.
- In Windows Defender Antivirus event logs, where a PUA event is recorded under event ID 1116 with the message: "The antimalware platform detected malware or other potentially unwanted software."

> **NOTE**
> Users will see "*.exe has been blocked as a potentially unwanted app by Microsoft Defender SmartScreen".

Allow-list an app

Like Microsoft Edge, Windows Defender Antivirus provides a way to allow files that are blocked by mistake or needed to complete a task. If this happens you can allow-list a file. For more information, see How to Configure Endpoint Protection in Configuration Manager to learn how to exclude specific files or folders.

See also

- Microsoft Edge Enterprise landing page
- Threat protection
- Configure behavioral, heuristic, and real-time protection
- Next-generation protection
- Security baseline for Chromium-based Microsoft Edge, version 79

Microsoft Edge and Conditional Access

11/1/2022 • 2 minutes to read • Edit Online

This article describes how Microsoft Edge supports Conditional Access, and how to access resources protected by Conditional Access.

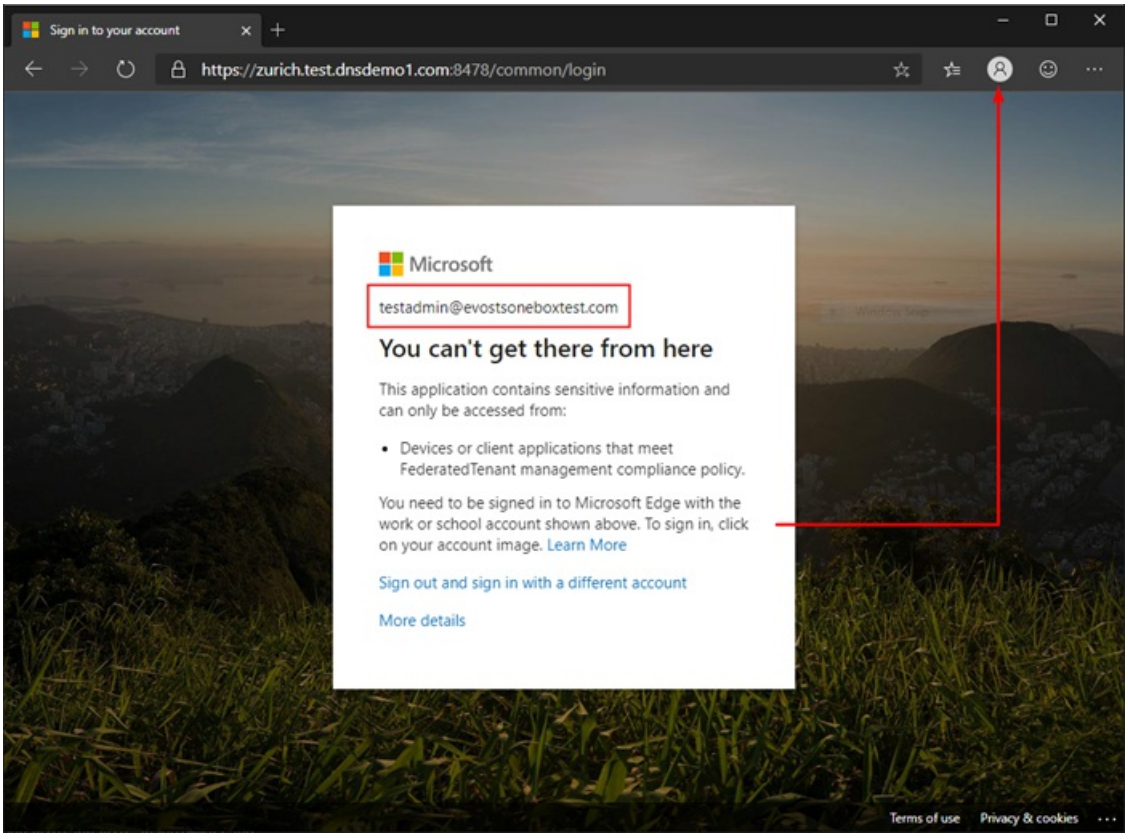
> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

A key aspect of cloud security is identity and access when it comes to managing your cloud resources. In a mobile-first, cloud-first world, users can access your organization's resources using various devices and apps from anywhere. As a result of this, just focusing on who can access a resource isn't sufficient. You also need to factor in how a resource is accessed. Azure Active Directory (Azure AD) Conditional Access helps you master the balance between security and productivity.

Accessing Conditional Access protected resources in Microsoft Edge

Microsoft Edge natively supports Azure AD Conditional Access. There's no need to install a separate extension. When you're signed into a Microsoft Edge profile with enterprise Azure AD credentials, Microsoft Edge allows seamless access to enterprise cloud resources protected using Conditional Access.

On a compliant device, the identity accessing the resource should match the identity on the profile. If it doesn't, you'll see a message like the one in the next screenshot. In the screenshot example, "testadmin@evostsoneboxtest.com" is the sign-in account needed to access the resource.


Sign in to your account
https://zurich.test.dnsdemo1.com:8478/common/login
Microsoft
testadmin@evostsoneboxtest.com
You can't get there from here
This application contains sensitive information and can only be accessed from:
Devices or client applications that meet FederatedTenant management compliance policy.
You need to be signed in to Microsoft Edge with the work or school account shown above. To sign in, click on your account image. Learn More
Sign out and sign in with a different account
More details
Terms of use
Privacy & cookies

To continue, you have to switch to the required profile (if you have one) or create a profile with matching identity.

To sign in and work with your profile, select the account picture in the top right corner of the browser. You can use the dropdown menu to:

- Pick another profile. Select the profile name.
- Create a profile. Select **Add a profile**.
- Manage your profiles. Select **Manage profile settings**.

This support is available across all platforms, including all supported versions of Windows and macOS.

> **NOTE**
> Conditional Access is not supported in InPrivate mode, as there's no concept of a signed in profile in this mode.

How to deploy Conditional Access in Azure Active Directory

Deploy Conditional Access provides a detailed guide to help plan and deploy Conditional Access in Azure Active Directory.

See also

- Microsoft Edge Enterprise landing page
- Video: Security, compatibility, and manageability

Microsoft Edge support for Microsoft Defender Application Guard

11/1/2022 • 8 minutes to read • Edit Online

This article describes how Microsoft Edge supports Microsoft Defender Application Guard (Application Guard).

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

Overview

Security architects in the enterprise must deal with the tension that exists between productivity and security. It's relatively easy to lock down a browser and only allow a handful of trusted sites to load. This approach will improve the overall security posture but is arguably less productive. If you make it less restrictive to improve productivity, you increase the risk profile. It's a hard balance to strike!

It's even harder to keep up with new emerging threats in this constantly changing threat landscape. Browsers remain the primary attack surface on client devices because the browser's basic job is to let users access, download, and open untrusted content from untrusted sources. Malicious actors are constantly working to social engineer new forms of attacks against the browser. Security incident prevention or detection/response strategies can't guarantee 100% safety.

A key security strategy to consider is the Assume Breach Methodology, which means there's an acceptance that an attack is going to succeed at least once regardless of efforts to prevent it. This mindset requires building defenses to contain the damage, which ensures that corporate network and other resources remain protected in this scenario. Deploying Application Guard for Microsoft Edge fits right into this strategy.

About Application Guard

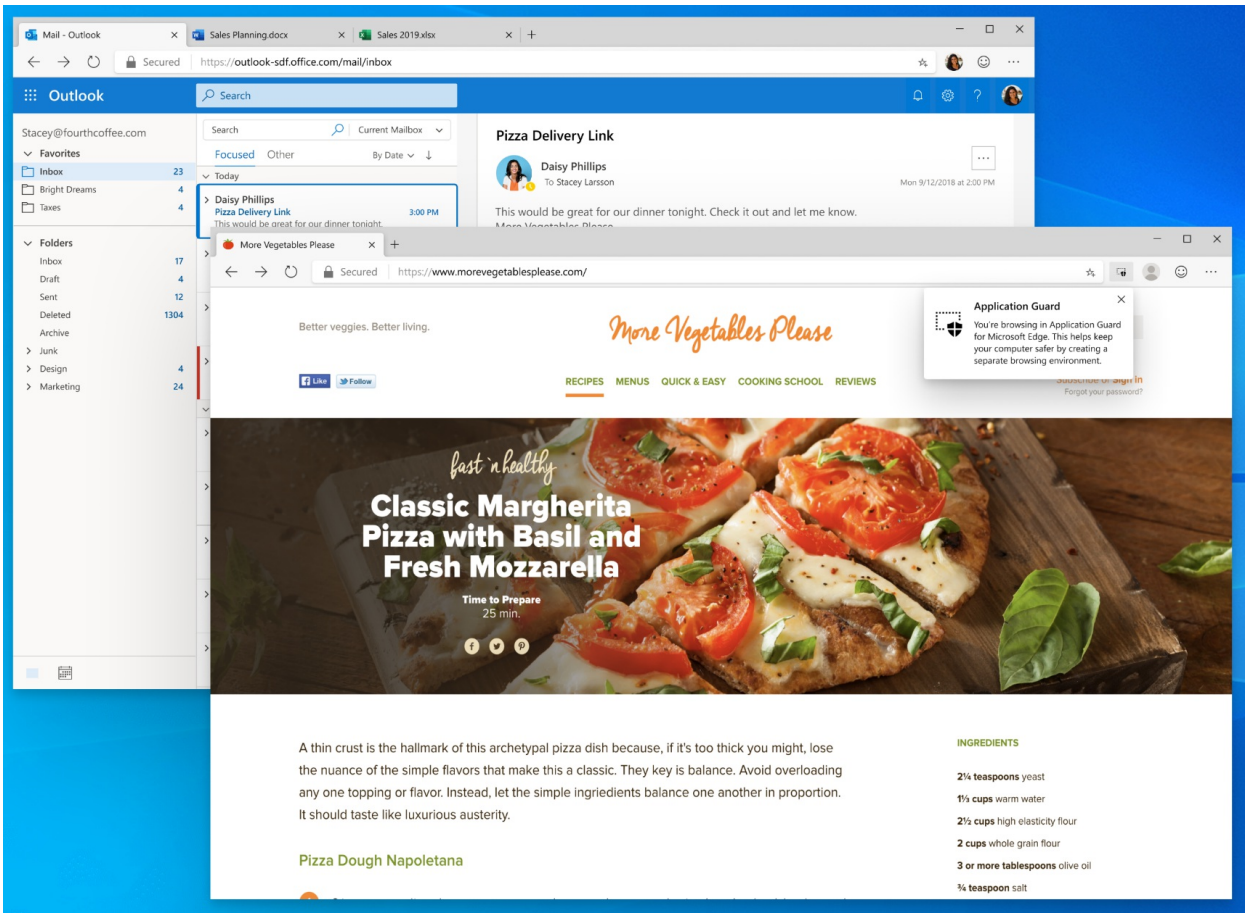
Designed for Windows 10 and Microsoft Edge, Application Guard uses a hardware isolation approach. This approach lets untrusted site navigation launch inside a container. Hardware isolation helps enterprises safeguard their corporate network and data in case users visit a site that is compromised or is malicious.

The enterprise administrator defines what are trusted sites, cloud resources, and internal networks. Everything that's not in the trusted sites list is considered untrusted. These sites are isolated from the corporate network and data on the user's device.

For more information:

- watch our video Microsoft Edge browser isolation using Application Guard
- read What is Application Guard and how does it work?

The next screenshot shows an example of Application Guard's message showing that the user is browsing in a safe space.


Mail - Outlook
Sales Planning.docx
Sales 2019.xlsx
Secured
https://outlook-sdf.office.com/mail/inbox
Outlook
Search
Stacey@fourthcoffee.com
Favorites
Inbox 23
Bright Dreams 4
Taxes 4
Folders
Inbox 17
Draft 4
Sent 12
Deleted 1304
Archive
Junk
Design 4
Marketing 24
Focused Other
Today
Daisy Phillips
Pizza Delivery Link
3:00 PM
Pizza Delivery Link
Daisy Phillips
To Stacey Larsson
Mon 9/12/2018 at 2:00 PM
This would be great for our dinner tonight. Check it out and let me know.
More Vegetables Please
https://www.morevegetablesplease.com/
Better veggies. Better living.
More Vegetables Please
RECIPES MENUS QUICK & EASY COOKING SCHOOL REVIEWS
Application Guard
You're browsing in Application Guard for Microsoft Edge. This helps keep your computer safer by creating a separate browsing environment.
fast 'n healthy
Classic Margherita Pizza with Basil and Fresh Mozzarella
Time to Prepare
25 min.
A thin crust is the hallmark of this archetypal pizza dish because, if it's too thick you might, lose the nuance of the simple flavors that make this a classic. They key is balance. Avoid overloading any one topping or flavor. Instead, let the simple ingriedients balance one another in proportion. It should taste like luxurious austerity.
Pizza Dough Napoletana
INGREDIENTS
2¼ teaspoons yeast
1½ cups warm water
2½ cups high elasticity flour
2 cups whole grain flour
3 or more tablespoons olive oil
¾ teaspoon salt

What's new

Application Guard support in the new Microsoft Edge browser has functional parity with Microsoft Edge Legacy and includes several improvements.

Enable Upload Blocking

Starting from Microsoft Edge 96, admins now have the option to block uploads while in the container, meaning that users cannot upload files from their local device to their Application Guard instance. This support can be controlled via policy. You can update the Edge policy ApplicationGuardUploadBlockingEnabled to enable or disable uploads in the container.

Enable Application Guard in passive mode and browse Edge normally

Starting from Microsoft Edge 94, users now have the option to configure passive mode, meaning that Application Guard ignores the site list configuration and users can browse Edge normally. This support can be controlled via policy. You can update the Edge policy ApplicationGuardPassiveModeEnabled to enable or disable passive mode.

> **NOTE**
> This policy ONLY impacts Edge, so navigations from other browsers might get redirected to the Application Guard Container if you have the corresponding extensions enabled.

Favorites synchronizing from the host to the container

Some of our customers have been asking for favorites sync between the host browser and the container in Application Guard. Starting from Microsoft Edge 91, users now have the option to configure Application Guard to synchronize their favorites from the host to the container. This ensures new favorites appear on the container as well.

This support can be controlled via policy. You can update the Edge policy ApplicationGuardFavoritesSyncEnabled

to enable or disable favorites sync.

> **NOTE**
> For security reasons, favorites sync is only possible from the host to the container and not the other way around. To ensure a unified list of favorites across the host and the container, we have disabled favorites management inside the container.

Identify network traffic originating from the container

Several customers are using WDAG in a specific configuration where they want to identify network traffic coming from the container. Some of the scenarios for this are:

- To restrict access to only a handful of untrusted sites
- To allow internet access from the container only

Starting with Microsoft Edge version 91, there's built in support to tag network traffic originating from Application Guard containers, allowing enterprises to use proxy to filter out traffic and apply specific policies. You can use the header to identify which traffic is through the container or the host using ApplicationGuardTrafficIdentificationEnabled.

Extension support inside the container

Extension support inside the container has been one of the top requests from the customers. Scenarios ranged from wanting to run ad-blockers inside the container to boost browser performance to having the ability to run custom home-grown extensions inside the container.

Extension installs in the container is now supported, starting from Microsoft Edge version 81. This support can be controlled via policy. The `updateURL` that gets used in ExtensionInstallForcelist policy should be added as Neutral Resources in the Network Isolation policies used by Application Guard.

Some examples of container support include the following scenarios:

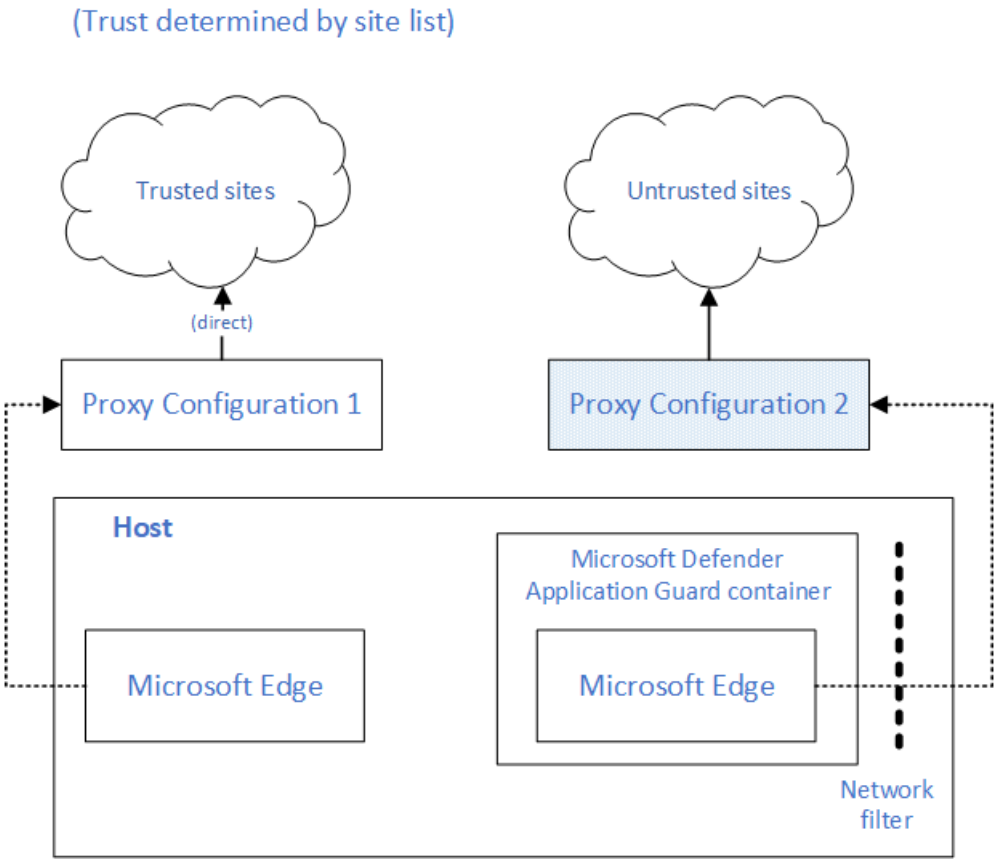
- Force installs of an extension on the host
- Removing an extension from the host
- Extensions blocked on the host

> **NOTE**
> It's also possible to manually install individual extensions inside the container from the extension store. Manually installed extensions will only persist in the container when Allow Persistence policy is enabled.

Identifying Application Guard traffic via Dual Proxy

Some enterprise customers are deploying Application Guard with a specific use case where they need to identify web traffic coming out of a Microsoft Defender Application Guard container at the proxy level. Starting with Stable Channel version 84, Microsoft Edge will support dual proxy to address this requirement. You can configure this functionality using the ApplicationGuardContainerProxy policy.

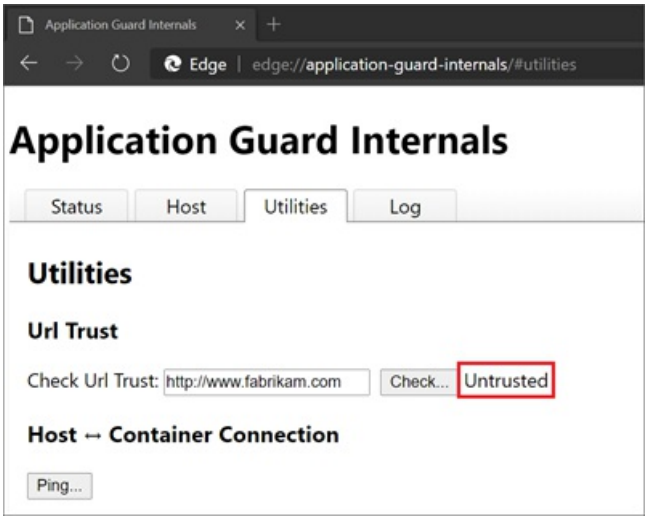
The following drawing shows the dual proxy architecture for Microsoft Edge.



Diagnostic page for troubleshooting

Another user pain point is troubleshooting the Application Guard configuration on a device when a problem is reported. Microsoft Edge has a diagnostics page (`edge://application-guard-internals`) to troubleshoot user issues. One of these diagnostics is being able to check the URL trust based on the configuration on the user's device.

The next screenshot shows a multiple tab diagnostics page to help diagnose user reported issues on the device.



Microsoft Edge updates in the container

Microsoft Edge Legacy updates in the container are part of the Windows OS update cycle. Because the new version of Microsoft Edge updates itself independent of the Windows OS, there is no longer any dependency on container updates. The channel and version of the host Microsoft Edge is replicated inside the container.

Prerequisites

The following requirements apply to devices using Application Guard with Microsoft Edge:

- Windows 10 1809 (RS5) and above.
- Only Windows client SKUs

> **NOTE**
> Application Guard is only supported on Windows 10 Pro and Windows 10 Enterprise SKUs.

- One of the management solutions described in Software requirements

How to install Application Guard

The following articles provide the information you need to install, configure, and test Application Guard with Microsoft Edge.

- System requirements
- Install Microsoft Defender Application Guard
- Configure Application Guard group policy settings
- Test Application Guard

Frequently Asked Questions

Does Application Guard work in IE mode?

IE mode supports Application Guard functionality, but we don't anticipate much use of this feature in IE Mode. IE mode is recommended to be deployed for a list of trusted internal sites, and Application Guard is for untrusted sites only. Make sure all the IE mode sites or IP addresses are also addedto the Network Isolation policy to be considered as trusted resource by Application Guard.

Do I need to install the Application Guard Chrome extension?

No, the Application Guard feature is natively supported in Microsoft Edge. In fact, the Application Guard Chrome extension isn't a supported configuration in Microsoft Edge.

Can employees download documents from the Application Guard Edge session onto host devices?

In Windows 10 Enterprise edition, version 1803, users are able to download documents from the isolated Application Guard container to the host PC. This capability is managed by policy.

In Windows 10 Enterprise edition, version 1709, or Windows 10 Professional edition, version 1803, it is not possible to download files from the isolated Application Guard container to the host computer. However, employees can use the Print as PDF or Print as XPS options and save those files to the host device.

Can employees copy and paste between the host device and the Application Guard Edge session?

Depending on your organization's settings, employees can copy and paste images (.bmp) and text to and from the isolated container.

Why don't employees see their favorites in the Application Guard Edge session?

Depending on your organization’s settings, it might be that Favorites Sync is turned off. To manage the policy, see: Microsoft Edge and Microsoft Defender Application Guard | Microsoft Docs.

Why aren’t employees able to see their extensions in the Application Guard Edge session?

Make sure to enable the extensions policy on your Application Guard configuration.

My extension doesn’t seem to work in Edge Application Guard?

If the extensions policy is enabled for MDAG in configuration, check if your extension requires Native Message Handling components, those extensions are not supported in the Application Guard container.

I'm trying to watch playback video with HDR, why is the HDR option missing?

In order for HDR video playback to work in the container, vGPU Hardware Acceleration needs to be enabled in Application Guard.

Are there any other platform related FAQs?

Yes. Frequently asked questions - Microsoft Defender Application Guard

See also

- Microsoft Edge Enterprise landing page
- Microsoft Defender Advanced Threat Protection
- Video: Microsoft Edge browser isolation using Application Guard

Microsoft Edge support for Microsoft Defender SmartScreen

11/1/2022 • 5 minutes to read • Edit Online

This article describes the benefits of using Microsoft Defender SmartScreen, explains how it works, and describes how to configure this Microsoft Edge feature.

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

Microsoft Defender SmartScreen is a service that Microsoft Edge uses to keep you safe while you browse the web. Microsoft Defender SmartScreen provides an early warning system against websites that might engage in phishing attacks or attempt to distribute malware through a focused attack. For more information, watch Video: Secure browsing on Microsoft Edge.

> **NOTE**
> Before Windows 10, version 1703, this feature was called the SmartScreen filter when used within the browser and Microsoft SmartScreen when used outside of the browser.

The benefits of Microsoft Defender SmartScreen

Microsoft Defender SmartScreen provides several benefits, which are summarized in the following list. These benefits are described in detail in the Microsoft Defender SmartScreen documentation. The benefits are:

- Anti-phishing and anti-malware support
- Reputation-based URL and app protection
- Operating system integration
- Improved heuristics and diagnostic data
- Management through Group Policy and Microsoft Intune
- Blocking URLs associated with potentially unwanted applications

Understand how Microsoft Defender SmartScreen works

A number of inputs contribute to Microsoft Defender SmartScreen warnings. Data is received from many sources, including user feedback, data providers, and intelligence models. This data is used to help identify potentially malicious content. Microsoft Defender SmartScreen also checks downloaded apps or app installers to see if they're malicious. In both scenarios, Microsoft Defender SmartScreen warns users appropriately about suspicious content.

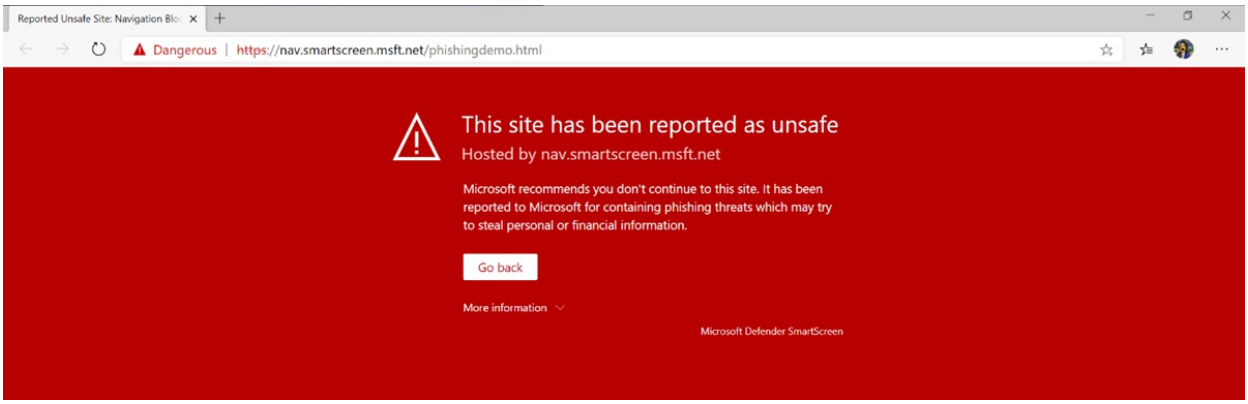
Site analysis

Microsoft Defender SmartScreen determines whether a site is potentially malicious by:

- Analyzing visited webpages for indications of suspicious behavior.
- Checking the visited sites against a dynamic record of reported phishing sites.

If Microsoft Defender SmartScreen determines that a page is malicious, it will show a warning page to notify the

user that that site is reported as unsafe. The next screenshot shows an example of a Microsoft Defender SmartScreen warning page when a user tries to open a malicious website.


Reported Unsafe Site: Navigation Blo
Dangerous | https://nav.smartscreen.msft.net/phishingdemo.html
This site has been reported as unsafe
Hosted by nav.smartscreen.msft.net
Microsoft recommends you don't continue to this site. It has been reported to Microsoft for containing phishing threats which may try to steal personal or financial information.
Go back
More information
Microsoft Defender SmartScreen

Users are given the option of reporting a site as safe or unsafe within the warning message. For more information, see how to report a site.

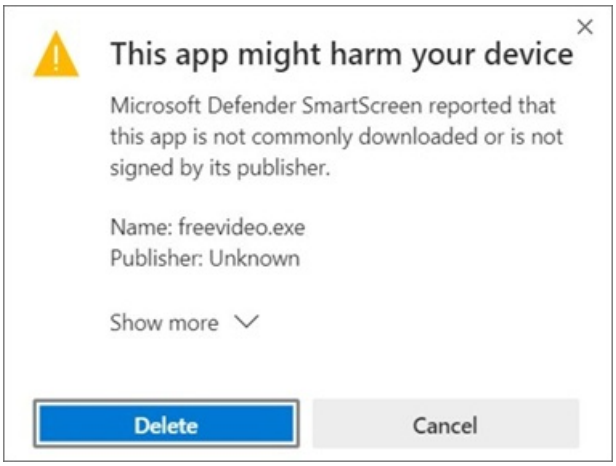
File analysis

Microsoft Defender SmartScreen determines whether a downloaded app or app installer is potentially malicious based on many criteria, such as download traffic, download history, past anti-virus results, and URL reputation.

- Files with a known safe reputation will download without any notification.
- Files with a known malicious reputation show a warning to let the user know that the file is unsafe and has been reported as malicious. The next screenshot is an example of a warning for a malicious file.

- Files that are unknown show a warning to let the user know that the download doesn't have a known footprint and advise caution. The next screenshot is an example of a warning for an unknown file.

Not all unknown programs are malicious, and the unknown warning is intended to provide context and guidance for users who need it, especially if the warning is unexpected.


This app might harm your device
Microsoft Defender SmartScreen reported that this app is not commonly downloaded or is not signed by its publisher.
Name: freevideo.exe
Publisher: Unknown
Show more
Delete
Cancel

However, users can still download and run the application by clicking **... | Keep | Show More | Keep anyway**.

> **TIP**
>
> **FYI for Enterprise Customers.** By default, Microsoft Defender SmartScreen lets users bypass warnings. Because this user interaction is potentially risky, we recommend that you review these recommended group policy settings.

You see how Microsoft Defender SmartScreen responds to different scenarios using our demo site.

Microsoft Defender SmartScreen and user privacy

Microsoft Defender SmartScreen protects users while they browse the Internet by using a reputation check system. Microsoft Edge passes relevant information about the URL or file to the Microsoft Defender SmartScreen service to start the reputation check. The check compares the website or file against dynamic lists of sites and files that are known to be dangerous. All requests to the Microsoft Defender SmartScreen service are made with TLS encryption. The service returns the results of the reputation check, which might lead to Microsoft Edge showing a warning for the site or file. These results are stored locally on the device.

The Microsoft Defender SmartScreen service stores data about reputation checks. As new sites are identified, the service adds to a dynamic database of known malicious URLs and files. This data is stored on secure Microsoft servers and is only used for Microsoft security services. This data will never be used to identify or target users in any way. Clearing browsing cache clears all locally stored Microsoft Defender SmartScreen URL data. Clearing download history will remove any locally stored SmartScreen data about file downloads.

For more information about Microsoft Defender SmartScreen and privacy on Microsoft Edge, read the Microsoft Edge Privacy Whitepaper.

Microsoft Defender SmartScreen setup for admins

Admins can configure Microsoft Defender SmartScreen using Group Policy, Microsoft Intune, or mobile device management (MDM) settings. Based on how you set up Microsoft Defender SmartScreen, you can show users a warning page and let them continue to the site or block the site entirely.

Microsoft Defender SmartScreen set up using Group Policy

For a complete list of SmartScreen policies, see Microsoft Defender SmartScreen settings

Microsoft Defender SmartScreen set up using MDM

For more information, see:

- Windows Intune settings for Microsoft Defender SmartScreen
- MDM policy settings

Microsoft Defender SmartScreen setup for users

Microsoft Defender SmartScreen is turned on by default for Microsoft Edge. To turn off Microsoft Defender SmartScreen, go to *edge://settings/privacy > Services > Microsoft Defender SmartScreen*. This setting is the same for all profiles associated with the installation of Microsoft Edge on a device. This setting is not synced across devices. The setting applies to InPrivate browsing and Guest mode. If a device is managed with group policies set by an organization, this configuration will be reflected in *edge://settings/privacy*.

> **NOTE**
>
> Users can set up Microsoft Defender SmartScreen for an individual device unless Group Policy or MDM is configured to prevent it. For more information, see set up and use Microsoft Defender SmartScreen on individual devices.

Frequently asked questions

How does the reputation check system work?

As you browse the web, Microsoft Defender SmartScreen categorizes websites and downloads as top traffic, dangerous, or unknown. Top traffic is popular sites that Microsoft Defender SmartScreen has determined are trustworthy. If you go to a site marked as dangerous, Microsoft Defender SmartScreen immediately blocks you from accessing the site. When you go to an unknown site, Microsoft DefenderSmartScreen checks its reputation to determine if you should access the site.

See also

- Microsoft Edge Enterprise landing page
- Video: Secure browsing on Microsoft Edge
- Microsoft Defender SmartScreen Overview
- Threat protection
- Protect against potentially unwanted applications

Microsoft Edge support for Windows Information Protection (WIP)

11/1/2022 • 4 minutes to read • Edit Online

This article describes how Microsoft Edge supports Windows Information Protection (WIP).

> **NOTE**
> This applies to Microsoft Edge version 81 or later. Windows information protection will be discontinued over time. For more information, see Announcing the sunset of Windows Information Protection (WIP).

Overview

Windows Information Protection (WIP) is a Windows 10 feature that helps protect enterprise data from unauthorized or accidental disclosure. With the rise of remote work, there's an increased risk of sharing corporate data outside the workplace. This risk increases when personal activities and work activities occur on corporate devices.

Microsoft Edge supports WIP to help protect content in a web environment where users often share and distribute content.

System requirements

The follow requirements apply to devices using WIP in the enterprise:

- Windows 10, version 1607 or later
- Only Windows client SKUs
- One of the management solutions described in WIP prerequisites

Windows Information Protection benefits

WIP provides the following benefits:

- Obvious separation between personal and corporate data, without requiring employees to switch environments or apps.
- Additional data protection for existing line-of-business apps without a need to update the apps.
- The ability to remote wipes corporate data from Intune Mobile Device Management (MDM) enrolled devices while leaving personal data unaffected.
- Audit reports for tracking issues and for remedial actions such as compliance training for users.
- Integration with your existing management system to configure, deploy, and manage WIP. Some examples are Microsoft Intune, Microsoft Endpoint Configuration Manager, or your current mobile device management (MDM) system.

WIP policy and protection modes

Using policies, you can configure the four protection modes described in the following table. For more information, see WIP-protection modes.

MODE	DESCRIPTION
Block	WIP looks for inappropriate data sharing practices and stops the employee from completing the action. This search can include sharing enterprise data to non-enterprise-protected apps in addition to sharing enterprise data between apps or attempting to share outside of your organization's network.
Allow Overrides	WIP looks for inappropriate data sharing, warning employees if they do something deemed potentially unsafe. However, this management mode lets the employee override the policy and share the data, logging the action to your audit log.
Silent	WIP runs silently, logging inappropriate data sharing, without stopping anything that would have been prompted for employee interaction while in Allow Overrides mode. Unallowed actions, like apps inappropriately trying to access a network resource or WIP-protected data, are still stopped.
Off	WIP is turned off and doesn't help to protect or audit your data. After you turn off WIP, an attempt is made to decrypt any WIP-tagged files on the locally attached drives. Your previous decryption and policy info isn't automatically reapplied if you turn WIP protection back on.

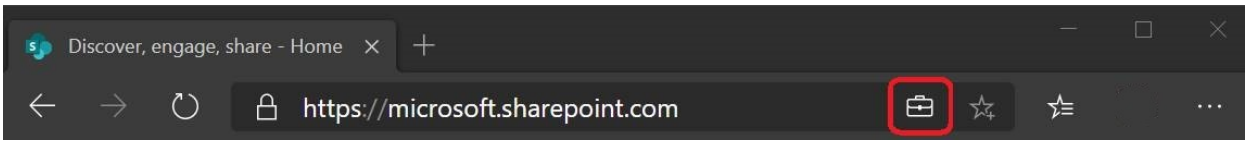
WIP features supported in Microsoft Edge

Starting with Microsoft Edge version 81, the following features are supported:

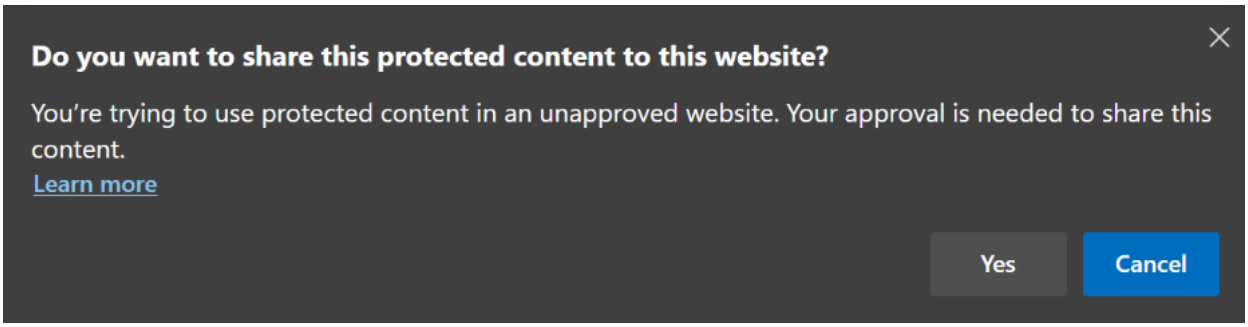
- Work sites will be indicated by a briefcase icon on the address bar.
- Files downloaded from a work location are automatically encrypted.
- Silent/Block/Override enforcement for work file uploads to non-work locations.
- Silent/Block/Override enforcement for file Drag & Drop actions.
- Silent/Block/Override enforcement for Clipboard actions.
- Browsing to work locations from non-work profiles automatically redirects to the Work Profile (associated with the Azure AD Identity.)
- IE Mode supports full WIP functionality.

Working with WIP in Microsoft Edge

After WIP support is enabled for Microsoft Edge, users will see when work-related information is accessed. The next screenshot shows the briefcase icon in the address bar, indicating that work-related information is accessed via the browser.



Microsoft Edge gives users the ability to share protected content in an unapproved website. The next screenshot shows the Microsoft Edge prompt that allows a user to use protected content in an unapproved website.


Do you want to share this protected content to this website?
You're trying to use protected content in an unapproved website. Your approval is needed to share this content.
Learn more
Yes
Cancel

Configure policies to support WIP

Using WIP with Microsoft Edge requires the presence of a work profile.

Ensure the presence of a work profile

On hybrid joined machines, Microsoft Edge is automatically signed in with the Azure Active Directory (Azure AD) account. To make sure that users don't remove this profile, which is needed for WIP, configure the following policy:

- NonRemovableProfileEnabled

> **NOTE**
> If your environment isn't hybrid joined, you can hybrid join using these instructions: Plan your hybrid Azure Active Directory join implementation.

If hybrid joining isn't an option, you can use on-prem Active Directory accounts to allow Microsoft Edge to auto create a special work profile with the users' domain accounts. Note that on-premises accounts may not receive all of Azure AD's features, such as cloud sync, Office NTP, and so on.)

Active Directory (AD) accounts

For AD accounts, you must configure the following policy to have the Microsoft Edge auto create a special work profile.

- ConfigureOnPremisesAccountAutoSignIn

Windows policies for WIP

You can configure WIP using Windows policies. For more information, see Create and deploy WIP policies using Microsoft Intune

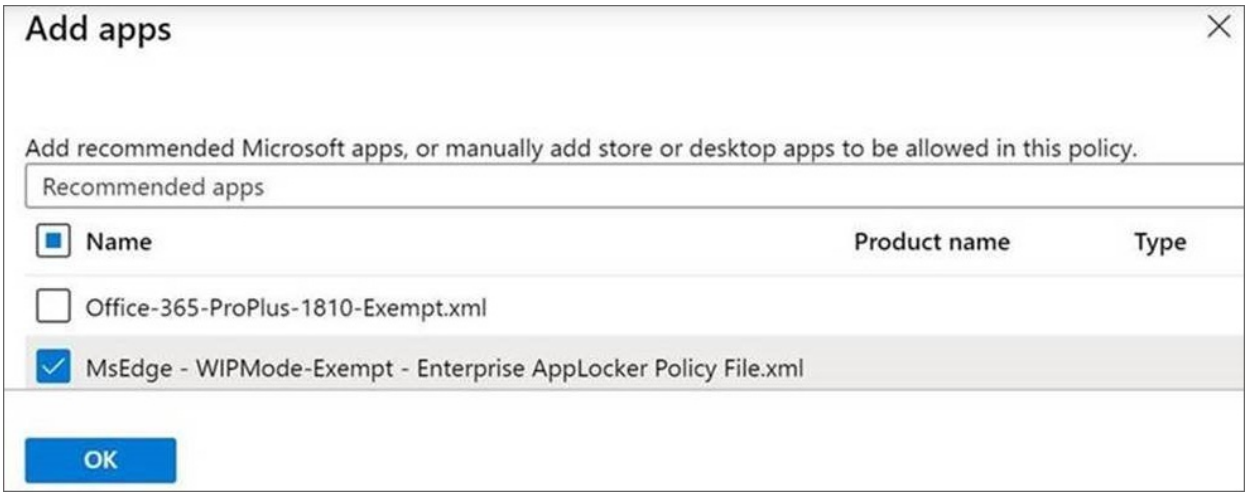
Frequently Asked Questions

How do I resolve Error Code -2147024540?

This error code corresponds to the following Windows Information Protection error:
ERROR_EDP_POLICY_DENIES_OPERATION: The requested operation was blocked by Windows Information Protection policy. For more information, contact your system administrator.

Microsoft Edge shows this error when the organization has enabled Windows Information Protection (WIP) to only allow users with approved applications to access corporate resources. In this case because Microsoft Edge isn't on the approved applications list, the admin will have to update the WIP policies to grant access to Microsoft Edge.

The following screenshot shows how the Microsoft Intune is used to add Microsoft Edge as an allowed app for WIP.



If you're not using Microsoft Intune, download and apply the policy update in the WIP Enterprise AppLocker Policy file.

See also

- Microsoft Edge Enterprise landing page
- Protect enterprise data using Windows Information Protection

Configure Microsoft Edge policies to support enterprise privacy

11/1/2022 • 5 minutes to read • Edit Online

Microsoft is committed to providing enterprises with the information and controls needed to make choices about data collection in Microsoft Edge.

Overview

When Microsoft Edge is deployed on Windows 10, the default is to send diagnostic data based on the users' Windows Diagnostic data setting.

When Microsoft Edge is deployed on non-Windows platforms, diagnostic data is collected according to the settings of the following group policies:

- (DEPRECATED) MetricsReportingEnabled - Enable usage and crash-related data reporting. This policy will be obsolete in Microsoft Edge version 89.
- (DEPRECATED) SendSiteInfoToImproveServices - Send site information to improve Microsoft services. This policy will be obsolete in Microsoft Edge version 89.

The preceding deprecated policies are replaced by Allow Telemetry on Windows 10, and DiagnosticData policy for all other platforms.

Configure policy settings

Before you begin, download and use the latest Microsoft Edge Policy Template (For more information, see Configure Microsoft Edge.)

Send required and optional diagnostic data about browser usage

If the DiagnosticData policy is configured, it takes precedence over MetricsReportingEnabledand SendSiteInfoToImproveServices.

Required and optional diagnostic data

Required diagnostic data is collected to keep Microsoft Edge secure, up to date and performing as expected.

Optional diagnostic data includes data about how you use the browser, websites you visit and crash reports to help keep Microsoft Edge secure, up to date, and performing as expected and is used to improve Microsoft Edge and other Microsoft products and services for all users.

> **NOTE**
> This policy isn't supported on Windows 10 devices. To control data collection on Windows 10, IT admins must use the Windows diagnostic data group policy. This policy will either be to **Allow Telemetry** or to **Allow Diagnostic Data**, depending on the version of Windows. Learn more about Windows 10 diagnostic data collection.

Use one of the following settings to configure **DiagnosticData**:

- Off (Not recommended) (0) turns off required and optional diagnostic data collection.
- Required data (1) sends required diagnostic data but turns off optional diagnostic data collection. Microsoft Edge will send required diagnostic data necessary to keep Microsoft Edge secure, up to date and performing as expected.

- Optional data (2) sends optional diagnostic data includes data about browser usage, websites that are visited, crash reports sent to Microsoft to help keep Microsoft Edge secure, up to date, and performing as expected and is used to improve Microsoft Edge and other Microsoft products and services for all users.

On Windows 7, Windows 8/8.1, and macOS, this policy controls sending required and optional data to Microsoft.

If you don't configure this policy or disable it Microsoft Edge will default to the user's preference.

(DEPRECATED) Enable usage and crash-related data reporting

The **MetricsReportingEnabled** policy enables reporting of usage and crash-related data about Microsoft Edge to Microsoft.

Microsoft Edge collects a set ofrequired datathat's necessary to keep the product up to date, secure, and performing as expected. This data includesbasic device connectivity and configuration information from Microsoft Edge about the current data collection consent, app version, and installation stateaboutyour installation of Microsoft Edge.This data collection can be turned off by disabling the policy.

Enable this policy to send reporting of usage and crash-related data to Microsoft. Disable this policy to not send the data to Microsoft. In both cases, users can't change or override the setting.

When Microsoft Edge is running on Windows 10:

- If this policy isn't configured, Microsoft Edge will default to the Windows diagnostic data setting.
- If this policy is enabled, Microsoft Edge will only send usage data if the Windows Diagnostic data setting is set to **Enhanced** or **Full**.
  - If this policy is enabled, Microsoft Edge will only send usage data if SendSiteInfoToImproveServices is also enabled.
- If this policy is disabled, Microsoft Edge will not send usage data. Crash-related data is sent based on the Windows Diagnostic data setting. Learn more about Windows Diagnostic data settings.

When Microsoft Edge is running on Windows 7, 8, and macOS:

- If this policy isn't configured, Microsoft Edge defaults to the user's preference.
- If this policy is enabled, Microsoft Edge will only send usage data if SendSiteInfoToImproveServices is also enabled.

(DEPRECATED) Send site information to improve Microsoft services

The **SendSiteInformationToImproveServices** policy enables sending information about websites visited in Microsoft Edge to Microsoft to improve Microsoft products and services such as search.

Enable this policy to send information about websites visited in Microsoft Edge to Microsoft. Disable this policy to not send information about the websites that are visited in Microsoft Edge to Microsoft. In both cases, users can't change or override the setting.

When Microsoft Edge is running on Windows 10:

- If this policy isn't configured, Microsoft Edge will default to the Windows diagnostic data setting.
- If this policy is enabled, Microsoft Edge will only send information about the websites that are visited if the Windows Diagnostic data setting is set to **Full**.
  - If this policy is enabled, Microsoft Edge will only send usage data if MetricsReportingEnabled is also enabled.
- If this policy is disabled, Microsoft Edge will not send info about websites visited. To learn more about Windows Diagnostic data settings.

When Microsoft Edge is running on Windows 7, 8, and macOS:

- If this policy is enabled, Microsoft Edge will only send usage data if MetricsReportingEnabled is also enabled.
- If this policy isn't configured, Microsoft Edge defaults to the user's preference.

Implementation details

For non-Windows 10 devices:

- If DiagnosticData policy is configured, it takes precedence over MetricsReportingEnabledand SendSiteInfoToImproveServices.
- If DiagnosticData policy isn't configured, Microsoft Edge listens to MetricsReportingEnabledand SendSiteInfoToImproveServices.

For Windows 10 to understand our implementation with the dependency on the Windows Diagnostic data setting, the following table identifies whether**Required** and **Optional** diagnostic data is sent to Microsoft.

WINDOWS DIAGNOSTIC DATA SETTING	REQUIRED DIAGNOSTIC DATA	OPTIONAL DIAGNOSTIC DATA
Security	Not sent	Not sent
Basic	Sent	Not sent
Enhanced	Sent	Not sent
Full	Sent	Sent

> **IMPORTANT**
> Microsoft Edge will support **MetricsReportingEnabled**and **SendSiteInfoToImproveServices** for Microsoft Edge versions 86 – 88 inclusive. In Microsoft Edge version 89, **MetricsReportingEnabled**and **SendSiteInfoToImproveServices** will no longer be supported and will default to **DiagnosticData** on non-Windows 10 platforms or the **Allow Telemetry** policy for Windows 10.

Additional privacy policy options

You may want to consider the following group policies related to data privacy:

- Block cookies on specific sites
- Block third-party cookies
- Configure Do Not Track
- Disable InPrivate mode

See also

- Microsoft Edge Enterprise landing page
- Microsoft Edge policies
- Microsoft Edge Privacy Whitepaper

Microsoft Edge - Policies

11/1/2022 • 570 minutes to read • Edit Online

The latest version of Microsoft Edge includes the following policies. You can use these policies to configure how Microsoft Edge runs in your organization.

For information about an additional set of policies used to control how and when Microsoft Edge is updated, check out Microsoft Edge update policy reference.

You can download the Microsoft Security Compliance Toolkit for the recommended security configuration baseline settings for Microsoft Edge. For more information see the Microsoft Security Baselines Blog.

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

New policies

The following table lists the new policies that are in this article update.

POLICY NAME	CAPTION
EncryptedClientHelloEnabled	TLS Encrypted ClientHello Enabled

Available policies

These tables list all of the browser-related group policies available in this release of Microsoft Edge. Use the links in the table to get more details about specific policies.

- Application Guard settings
- Cast
- Content settings
- Default search provider
- Edge Workspaces settings
- Experimentation
- Extensions
- HTTP authentication
- Identity and sign-in
- Kiosk Mode settings
- Manageability
- Native Messaging
- Password manager and protection
- Performance
- Permit or deny screen capture
- Printing
- Private Network Request Settings
- Proxy server

- Sleeping tabs settings
- SmartScreen settings
- Startup, home page and new tab page
- TyposquattingChecker settings
- Additional

Application Guard settings

POLICY NAME	CAPTION
ApplicationGuardContainerProxy	Application Guard Container Proxy
ApplicationGuardFavoritesSyncEnabled	Application Guard Favorites Sync Enabled
ApplicationGuardPassiveModeEnabled	Ignore Application Guard site list configuration and browse Edge normally
ApplicationGuardTrafficIdentificationEnabled	Application Guard Traffic Identification
ApplicationGuardUploadBlockingEnabled	Prevents files from being uploaded while in Application Guard

Cast

POLICY NAME	CAPTION
EnableMediaRouter	Enable Google Cast
ShowCastIconInToolbar	Show the cast icon in the toolbar

Content settings

POLICY NAME	CAPTION
AutoSelectCertificateForUrls	Automatically select client certificates for these sites
CookiesAllowedForUrls	Allow cookies on specific sites
CookiesBlockedForUrls	Block cookies on specific sites
CookiesSessionOnlyForUrls	Limit cookies from specific websites to the current session
DefaultCookiesSetting	Configure cookies
DefaultFileSystemReadGuardSetting	Control use of the File System API for reading
DefaultFileSystemWriteGuardSetting	Control use of the File System API for writing
DefaultGeolocationSetting	Default geolocation setting
DefaultImagesSetting	Default images setting
DefaultInsecureContentSetting	Control use of insecure content exceptions

POLICY NAME	CAPTION
DefaultJavaScriptJitSetting	Control use of JavaScript JIT
DefaultJavaScriptSetting	Default JavaScript setting
DefaultNotificationsSetting	Default notification setting
DefaultPluginsSetting	Default Adobe Flash setting (obsolete)
DefaultPopupsSetting	Default pop-up window setting
DefaultWebBluetoothGuardSetting	Control use of the Web Bluetooth API
DefaultWebHidGuardSetting	Control use of the WebHID API
DefaultWebUsbGuardSetting	Control use of the WebUSB API
FileSystemReadAskForUrls	Allow read access via the File System API on these sites
FileSystemReadBlockedForUrls	Block read access via the File System API on these sites
FileSystemWriteAskForUrls	Allow write access to files and directories on these sites
FileSystemWriteBlockedForUrls	Block write access to files and directories on these sites
ImagesAllowedForUrls	Allow images on these sites
ImagesBlockedForUrls	Block images on specific sites
InsecureContentAllowedForUrls	Allow insecure content on specified sites
InsecureContentBlockedForUrls	Block insecure content on specified sites
IntranetFileLinksEnabled	Allow intranet zone file URL links from Microsoft Edge to open in Windows File Explorer
JavaScriptAllowedForUrls	Allow JavaScript on specific sites
JavaScriptBlockedForUrls	Block JavaScript on specific sites
JavaScriptJitAllowedForSites	Allow JavaScript to use JIT on these sites
JavaScriptJitBlockedForSites	Block JavaScript from using JIT on these sites
LegacySameSiteCookieBehaviorEnabled	Enable default legacy SameSite cookie behavior setting (obsolete)
LegacySameSiteCookieBehaviorEnabledForDomainList	Revert to legacy SameSite behavior for cookies on specified sites
NotificationsAllowedForUrls	Allow notifications on specific sites

POLICY NAME	CAPTION
NotificationsBlockedForUrls	Block notifications on specific sites
PluginsAllowedForUrls	Allow the Adobe Flash plug-in on specific sites (obsolete)
PluginsBlockedForUrls	Block the Adobe Flash plug-in on specific sites (obsolete)
PopupsAllowedForUrls	Allow pop-up windows on specific sites
PopupsBlockedForUrls	Block pop-up windows on specific sites
RegisteredProtocolHandlers	Register protocol handlers
SerialAllowAllPortsForUrls	Automatically grant sites permission to connect all serial ports
SerialAllowUsbDevicesForUrls	Automatically grant sites permission to connect to USB serial devices
ShowPDFDefaultRecommendationsEnabled	Allow notifications to set Microsoft Edge as default PDF reader
SpotlightExperiencesAndRecommendationsEnabled	Choose whether users can receive customized background images and text, suggestions, notifications, and tips for Microsoft services
WebHidAskForUrls	Allow the WebHID API on these sites
WebHidBlockedForUrls	Block the WebHID API on these sites
WebUsbAllowDevicesForUrls	Grant access to specific sites to connect to specific USB devices
WebUsbAskForUrls	Allow WebUSB on specific sites
WebUsbBlockedForUrls	Block WebUSB on specific sites

Default search provider

POLICY NAME	CAPTION
DefaultSearchProviderEnabled	Enable the default search provider
DefaultSearchProviderEncodings	Default search provider encodings
DefaultSearchProviderImageURL	Specifies the search-by-image feature for the default search provider
DefaultSearchProviderImageURLPostParams	Parameters for an image URL that uses POST
DefaultSearchProviderKeyword	Default search provider keyword
DefaultSearchProviderName	Default search provider name

POLICY NAME	CAPTION
DefaultSearchProviderSearchURL	Default search provider search URL
DefaultSearchProviderSuggestURL	Default search provider URL for suggestions
NewTabPageSearchBox	Configure the new tab page search box experience

Edge Workspaces settings

POLICY NAME	CAPTION
EdgeWorkspacesEnabled	Enable Workspaces

Experimentation

POLICY NAME	CAPTION
FeatureFlagOverridesControl	Configure users ability to override feature flags

Extensions

POLICY NAME	CAPTION
BlockExternalExtensions	Blocks external extensions from being installed
ControlDefaultStateOfAllowExtensionFromOtherStoresSettingEnabled	Configure default state of Allow extensions from other stores setting
ExtensionAllowedTypes	Configure allowed extension types
ExtensionInstallAllowlist	Allow specific extensions to be installed
ExtensionInstallBlocklist	Control which extensions cannot be installed
ExtensionInstallForcelist	Control which extensions are installed silently
ExtensionInstallSources	Configure extension and user script install sources
ExtensionSettings	Configure extension management settings

HTTP authentication

POLICY NAME	CAPTION
AllHttpAuthSchemesAllowedForOrigins	List of origins that allow all HTTP authentication
AllowCrossOriginAuthPrompt	Allow cross-origin HTTP Authentication prompts
AuthNegotiateDelegateAllowlist	Specifies a list of servers that Microsoft Edge can delegate user credentials to
AuthSchemes	Supported authentication schemes

POLICY NAME	CAPTION
AuthServerAllowlist	Configure list of allowed authentication servers
BasicAuthOverHttpEnabled	Allow Basic authentication for HTTP
DisableAuthNegotiateCnameLookup	Disable CNAME lookup when negotiating Kerberos authentication
EnableAuthNegotiatePort	Include non-standard port in Kerberos SPN
NtlmV2Enabled	Control whether NTLMv2 authentication is enabled
WindowsHelloForHTTPAuthEnabled	Windows Hello For HTTP Auth Enabled

Identity and sign-in

POLICY NAME	CAPTION
EdgeDefaultProfileEnabled	Default Profile Setting Enabled
GuidedSwitchEnabled	Guided Switch Enabled
ImplicitSignInEnabled	Enable implicit sign-in
LinkedAccountEnabled	Enable the linked account feature
OneAuthAuthenticationEnforced	OneAuth Authentication Flow Enforced for signin
OnlyOnPremisesImplicitSigninEnabled	Only on-premises account enabled for implicit sign-in
SignInCtaOnNtpEnabled	Enable sign in click to action dialog
WAMAuthBelowWin10RS3Enabled	WAM for authentication below Windows 10 RS3 enabled

Kiosk Mode settings

POLICY NAME	CAPTION
KioskAddressBarEditingEnabled	Configure address bar editing for kiosk mode public browsing experience
KioskDeleteDownloadsOnExit	Delete files downloaded as part of kiosk session when Microsoft Edge closes
KioskSwipeGesturesEnabled	Swipe gestures in Microsoft Edge kiosk mode enabled

Manageability

POLICY NAME	CAPTION
MAMEnabled	Mobile App Management Enabled

Native Messaging

POLICY NAME	CAPTION
NativeMessagingAllowlist	Control which native messaging hosts users can use
NativeMessagingBlocklist	Configure native messaging block list
NativeMessagingUserLevelHosts	Allow user-level native messaging hosts (installed without admin permissions)

Password manager and protection

POLICY NAME	CAPTION
PasswordGeneratorEnabled	Allow users to get a strong password suggestion whenever they are creating an account online
PasswordManagerBlocklist	Configure the list of domains for which the password manager UI (Save and Fill) will be disabled
PasswordManagerEnabled	Enable saving passwords to the password manager
PasswordManagerRestrictLengthEnabled	Restrict the length of passwords that can be saved in the Password Manager
PasswordMonitorAllowed	Allow users to be alerted if their passwords are found to be unsafe
PasswordProtectionChangePasswordURL	Configure the change password URL
PasswordProtectionLoginURLs	Configure the list of enterprise login URLs where the password protection service should capture salted hashes of a password
PasswordProtectionWarningTrigger	Configure password protection warning trigger
PasswordRevealEnabled	Enable Password reveal button
PrimaryPasswordSetting	Configures a setting that asks users to enter their device password while using password autofill

Performance

POLICY NAME	CAPTION
EfficiencyMode	Configure when efficiency mode should become active
EfficiencyModeEnabled	Efficiency mode enabled
EfficiencyModeOnPowerEnabled	Enable efficiency mode when the device is connected to a power source
PerformanceDetectorEnabled	Performance Detector Enabled
StartupBoostEnabled	Enable startup boost

Permit or deny screen capture

POLICY NAME	CAPTION
SameOriginTabCaptureAllowedByOrigins	Allow Same Origin Tab capture by these origins
ScreenCaptureAllowedByOrigins	Allow Desktop, Window, and Tab capture by these origins
TabCaptureAllowedByOrigins	Allow Tab capture by these origins
WindowCaptureAllowedByOrigins	Allow Window and Tab capture by these origins

Printing

POLICY NAME	CAPTION
DefaultPrinterSelection	Default printer selection rules
PrintHeaderFooter	Print headers and footers
PrintPdfAsImageDefault	Print PDF as Image Default
PrintPostScriptMode	Print PostScript Mode
PrintPreviewUseSystemDefaultPrinter	Set the system default printer as the default printer
PrintRasterizationMode	Print Rasterization Mode
PrintRasterizePdfDpi	Print Rasterize PDF DPI
PrintStickySettings	Print preview sticky settings
PrinterTypeDenyList	Disable printer types on the deny list
PrintingAllowedBackgroundGraphicsModes	Restrict background graphics printing mode
PrintingBackgroundGraphicsDefault	Default background graphics printing mode
PrintingEnabled	Enable printing
PrintingPaperSizeDefault	Default printing page size
PrintingWebpageLayout	Sets layout for printing
UseSystemPrintDialog	Print using system print dialog

Private Network Request Settings

POLICY NAME	CAPTION
InsecurePrivateNetworkRequestsAllowed	Specifies whether to allow insecure websites to make requests to more-private network endpoints

POLICY NAME	CAPTION
InsecurePrivateNetworkRequestsAllowedForUrls	Allow the listed sites to make requests to more-private network endpoints from insecure contexts

Proxy server

POLICY NAME	CAPTION
ProxyBypassList	Configure proxy bypass rules (deprecated)
ProxyMode	Configure proxy server settings (deprecated)
ProxyPacUrl	Set the proxy .pac file URL (deprecated)
ProxyServer	Configure address or URL of proxy server (deprecated)
ProxySettings	Proxy settings

Sleeping tabs settings

POLICY NAME	CAPTION
SleepingTabsBlockedForUrls	Block sleeping tabs on specific sites
SleepingTabsEnabled	Configure sleeping tabs
SleepingTabsTimeout	Set the background tab inactivity timeout for sleeping tabs

SmartScreen settings

POLICY NAME	CAPTION
NewSmartScreenLibraryEnabled	Enable new SmartScreen library (obsolete)
PreventSmartScreenPromptOverride	Prevent bypassing Microsoft Defender SmartScreen prompts for sites
PreventSmartScreenPromptOverrideForFiles	Prevent bypassing of Microsoft Defender SmartScreen warnings about downloads
SmartScreenAllowListDomains	Configure the list of domains for which Microsoft Defender SmartScreen won't trigger warnings
SmartScreenDnsRequestsEnabled	Enable Microsoft Defender SmartScreen DNS requests
SmartScreenEnabled	Configure Microsoft Defender SmartScreen
SmartScreenForTrustedDownloadsEnabled	Force Microsoft Defender SmartScreen checks on downloads from trusted sources
SmartScreenPuaEnabled	Configure Microsoft Defender SmartScreen to block potentially unwanted apps

Startup, home page and new tab page

POLICY NAME	CAPTION
HomepageIsNewTabPage	Set the new tab page as the home page
HomepageLocation	Configure the home page URL
NewTabPageAllowedBackgroundTypes	Configure the background types allowed for the new tab page layout
NewTabPageAppLauncherEnabled	Hide App Launcher on Microsoft Edge new tab page
NewTabPageCompanyLogo	Set new tab page company logo (obsolete)
NewTabPageContentEnabled	Allow Microsoft News content on the new tab page
NewTabPageHideDefaultTopSites	Hide the default top sites from the new tab page
NewTabPageLocation	Configure the new tab page URL
NewTabPageManagedQuickLinks	Set new tab page quick links
NewTabPagePrerenderEnabled	Enable preload of the new tab page for faster rendering
NewTabPageQuickLinksEnabled	Allow quick links on the new tab page
NewTabPageSetFeedType	Configure the Microsoft Edge new tab page experience (obsolete)
RestoreOnStartup	Action to take on startup
RestoreOnStartupURLs	Sites to open when the browser starts
RestoreOnStartupUserURLsEnabled	Allow users to add and remove their own sites during startup when the RestoreOnStartupURLs policy is configured
ShowHomeButton	Show Home button on toolbar

TyposquattingChecker settings

POLICY NAME	CAPTION
TyposquattingCheckerEnabled	Configure Edge TyposquattingChecker

Additional

POLICY NAME	CAPTION
AADWebSiteSSOUsingThisProfileEnabled	Single sign-on for work or school sites using this profile enabled
AccessibilityImageLabelsEnabled	Let screen reader users get image descriptions from Microsoft

POLICY NAME	CAPTION
AddressBarEditingEnabled	Configure address bar editing
AddressBarMicrosoftSearchInBingProviderEnabled	Enable Microsoft Search in Bing suggestions in the address bar
AdsSettingForIntrusiveAdsSites	Ads setting for sites with intrusive ads
AdsTransparencyEnabled	Configure if the ads transparency feature is enabled
AllowDeletingBrowserHistory	Enable deleting browser and download history
AllowFileSelectionDialogs	Allow file selection dialogs
AllowGamesMenu	Allow users to access the games menu
AllowPopupsDuringPageUnload	Allows a page to show popups during its unloading (obsolete)
AllowSurfGame	Allow surf game
AllowSyncXHRInPageDismissal	Allow pages to send synchronous XHR requests during page dismissal (obsolete)
AllowTokenBindingForUrls	Configure the list of sites for which Microsoft Edge will attempt to establish a Token Binding with
AllowTrackingForUrls	Configure tracking prevention exceptions for specific sites
AllowedDomainsForApps	Define domains allowed to access Google Workspace
AlternateErrorPagesEnabled	Suggest similar pages when a webpage can't be found
AlwaysOpenPdfExternally	Always open PDF files externally
AmbientAuthenticationInPrivateModesEnabled	Enable Ambient Authentication for InPrivate and Guest profiles
AppCacheForceEnabled	Allows the AppCache feature to be re-enabled, even if it's turned off by default (obsolete)
ApplicationLocaleValue	Set application locale
AskBeforeCloseEnabled	Get user confirmation before closing a browser window with multiple tabs
AudioCaptureAllowed	Allow or block audio capture
AudioCaptureAllowedUrls	Sites that can access audio capture devices without requesting permission
AudioProcessHighPriorityEnabled	Allow the audio process to run with priority above normal on Windows

POLICY NAME	CAPTION
AudioSandboxEnabled	Allow the audio sandbox to run
AutoImportAtFirstRun	Automatically import another browser's data and settings at first run
AutoLaunchProtocolsComponentEnabled	AutoLaunch Protocols Component Enabled
AutoLaunchProtocolsFromOrigins	Define a list of protocols that can launch an external application from listed origins without prompting the user
AutoOpenAllowedForURLs	URLs where AutoOpenFileTypes can apply
AutoOpenFileTypes	List of file types that should be automatically opened on download
AutofillAddressEnabled	Enable AutoFill for addresses
AutofillCreditCardEnabled	Enable AutoFill for payment instruments
AutomaticHttpsDefault	Configure Automatic HTTPS
AutoplayAllowed	Allow media autoplay for websites
AutoplayAllowlist	Allow media autoplay on specific sites
BackgroundModeEnabled	Continue running background apps after Microsoft Edge closes
BackgroundTemplateListUpdatesEnabled	Enables background updates to the list of available templates for Collections and other features that use templates (deprecated)
BingAdsSuppression	Block all ads on Bing search results
BlockThirdPartyCookies	Block third party cookies
BrowserAddProfileEnabled	Enable profile creation from the Identity flyout menu or the Settings page
BrowserCodeIntegritySetting	Configure browser process code integrity guard setting
BrowserGuestModeEnabled	Enable guest mode
BrowserLegacyExtensionPointsBlockingEnabled	Enable browser legacy extension point blocking
BrowserNetworkTimeQueriesEnabled	Allow queries to a Browser Network Time service
BrowserSignin	Browser sign-in settings
BrowsingDataLifetime	Browsing Data Lifetime Settings

POLICY NAME	CAPTION
BuiltInDnsClientEnabled	Use built-in DNS client
BuiltinCertificateVerifierEnabled	Determines whether the built-in certificate verifier will be used to verify server certificates (obsolete)
CECPQ2Enabled	CECPQ2 post-quantum key-agreement enabled for TLS
CORSNonWildcardRequestHeadersSupport	CORS non-wildcard request header support enabled
CertificateTransparencyEnforcementDisabledForCas	Disable Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes
CertificateTransparencyEnforcementDisabledForLegacyCas	Disable Certificate Transparency enforcement for a list of legacy certificate authorities
CertificateTransparencyEnforcementDisabledForUrls	Disable Certificate Transparency enforcement for specific URLs
ClearBrowsingDataOnExit	Clear browsing data when Microsoft Edge closes
ClearCachedImagesAndFilesOnExit	Clear cached images and files when Microsoft Edge closes
ClickOnceEnabled	Allow users to open files using the ClickOnce protocol
CollectionsServicesAndExportsBlockList	Block access to a specified list of services and export targets in Collections
CommandLineFlagSecurityWarningsEnabled	Enable security warnings for command-line flags
ComponentUpdatesEnabled	Enable component updates in Microsoft Edge
ConfigureDoNotTrack	Configure Do Not Track
ConfigureFriendlyURLFormat	Configure the default paste format of URLs copied from Microsoft Edge, and determine if additional formats will be available to users
ConfigureKeyboardShortcuts	Configure the list of commands for which to disable keyboard shortcuts
ConfigureOnPremisesAccountAutoSignIn	Configure automatic sign in with an Active Directory domain account when there is no Azure AD domain account
ConfigureOnlineTextToSpeech	Configure Online Text To Speech
ConfigureShare	Configure the Share experience
ConfigureViewInFileExplorer	Configure the View in File Explorer feature for SharePoint pages in Microsoft Edge
CrossOriginWebAssemblyModuleSharingEnabled	Specifies whether WebAssembly modules can be sent cross-origin (obsolete)

POLICY NAME	CAPTION
CustomHelpLink	Specify custom help link
DNSInterceptionChecksEnabled	DNS interception checks enabled
DefaultBrowserSettingEnabled	Set Microsoft Edge as default browser
DefaultSearchProviderContextMenuAccessAllowed	Allow default search provider context menu search access
DefaultSensorsSetting	Default sensors setting
DefaultSerialGuardSetting	Control use of the Serial API
DefaultShareAdditionalOSRegionSetting	Set the default "share additional operating system region" setting
DefinePreferredLanguages	Define an ordered list of preferred languages that websites should display in if the site supports the language
DelayNavigationsForInitialSiteListDownload	Require that the Enterprise Mode Site List is available before tab navigation
DeleteDataOnMigration	Delete old browser data on migration
DeveloperToolsAvailability	Control where developer tools can be used
DiagnosticData	Send required and optional diagnostic data about browser usage
DirectInvokeEnabled	Allow users to open files using the DirectInvoke protocol
Disable3DAPIs	Disable support for 3D graphics APIs
DisableScreenshots	Disable taking screenshots
DiskCacheDir	Set disk cache directory
DiskCacheSize	Set disk cache size, in bytes
DisplayCapturePermissionsPolicyEnabled	Specifies whether the display-capture permissions-policy is checked or skipped
DnsOverHttpsMode	Control the mode of DNS-over-HTTPS
DnsOverHttpsTemplates	Specify URI template of desired DNS-over-HTTPS resolver
DoNotSilentlyBlockProtocolsFromOrigins	Define a list of protocols that can not be silently blocked by anti-flood protection
DoubleClickCloseTabEnabled	Double Click feature in Microsoft Edge enabled (only available in China)

POLICY NAME	CAPTION
DownloadDirectory	Set download directory
DownloadRestrictions	Allow download restrictions
EdgeAssetDeliveryServiceEnabled	Allow features to download assets from the Asset Delivery Service
EdgeCollectionsEnabled	Enable the Collections feature
EdgeDiscoverEnabled	Discover feature In Microsoft Edge (obsolete)
EdgeEDropEnabled	Enable Drop feature in Microsoft Edge
EdgeEnhanceImagesEnabled	Enhance images enabled
EdgeFollowEnabled	Enable Follow service in Microsoft Edge
EdgeShoppingAssistantEnabled	Shopping in Microsoft Edge Enabled
EditFavoritesEnabled	Allows users to edit favorites
EnableDeprecatedWebPlatformFeatures	Re-enable deprecated web platform features for a limited time (obsolete)
EnableDomainActionsDownload	Enable Domain Actions Download from Microsoft (obsolete)
EnableOnlineRevocationChecks	Enable online OCSP/CRL checks
EnableSha1ForLocalAnchors	Allow certificates signed using SHA-1 when issued by local trust anchors (obsolete)
EncryptedClientHelloEnabled	TLS Encrypted ClientHello Enabled
EnhanceSecurityMode	Enhance the security state in Microsoft Edge
EnhanceSecurityModeBypassIntranet	Enhanced Security Mode configuration for Intranet zone sites
EnhanceSecurityModeBypassListDomains	Configure the list of domains for which enhance security mode will not be enforced
EnhanceSecurityModeEnforceListDomains	Configure the list of domains for which enhance security mode will always be enforced
EnterpriseHardwarePlatformAPIEnabled	Allow managed extensions to use the Enterprise Hardware Platform API
EnterpriseModeSiteListManagerAllowed	Allow access to the Enterprise Mode Site List Manager tool
EventPathEnabled	Re-enable the Event.path API until Microsoft Edge version 115

POLICY NAME	CAPTION
ExemptDomainFileTypePairsFromFileTypeDownloadWarnings	Disable download file type extension-based warnings for specified file types on domains (deprecated)
ExemptFileTypeDownloadWarnings	Disable download file type extension-based warnings for specified file types on domains
ExperimentationAndConfigurationServiceControl	Control communication with the Experimentation and Configuration Service
ExplicitlyAllowedNetworkPorts	Explicitly allowed network ports
ExternalProtocolDialogShowAlwaysOpenCheckbox	Show an "Always open" checkbox in external protocol dialog
FamilySafetySettingsEnabled	Allow users to configure Family safety and Kids Mode
FavoritesBarEnabled	Enable favorites bar
FetchKeepaliveDurationSecondsOnShutdown	Fetch keepalive duration on shutdown
ForceBingSafeSearch	Enforce Bing SafeSearch
ForceCertificatePromptsOnMultipleMatches	Configure whether Microsoft Edge should automatically select a certificate when there are multiple certificate matches for a site configured with "AutoSelectCertificateForUrls" (deprecated)
ForceEphemeralProfiles	Enable use of ephemeral profiles
ForceGoogleSafeSearch	Enforce Google SafeSearch
ForceLegacyDefaultReferrerPolicy	Use a default referrer policy of no-referrer-when-downgrade (obsolete)
ForceMajorVersionToMinorPositionInUserAgent	Enable or disable freezing the User-Agent string at major version 99
ForceNetworkInProcess	Force networking code to run in the browser process (obsolete)
ForceSync	Force synchronization of browser data and do not show the sync consent prompt
ForceSyncTypes	Configure the list of types that are included for synchronization
ForceYouTubeRestrict	Force minimum YouTube Restricted Mode
FullscreenAllowed	Allow full screen mode
GloballyScopeHTTPAuthCacheEnabled	Enable globally scoped HTTP auth cache

POLICY NAME	CAPTION
GoToIntranetSiteForSingleWordEntryInAddressBar	Force direct intranet site navigation instead of searching on single word entries in the Address Bar
HSTSPolicyBypassList	Configure the list of names that will bypass the HSTS policy check
HardwareAccelerationModeEnabled	Use hardware acceleration when available
HeadlessModeEnabled	Control use of the Headless Mode
HideFirstRunExperience	Hide the First-run experience and splash screen
HideInternetExplorerRedirectUXForIncompatibleSitesEnabled	Hide the one-time redirection dialog and the banner on Microsoft Edge
HideRestoreDialogEnabled	Hide restore pages dialog after browser crash
HubsSidebarEnabled	Show Hubs Sidebar
ImportAutofillFormData	Allow importing of autofill form data
ImportBrowserSettings	Allow importing of browser settings
ImportCookies	Allow importing of Cookies
ImportExtensions	Allow importing of extensions
ImportFavorites	Allow importing of favorites
ImportHistory	Allow importing of browsing history
ImportHomepage	Allow importing of home page settings
ImportOnEachLaunch	Allow import of data from other browsers on each Microsoft Edge launch
ImportOpenTabs	Allow importing of open tabs
ImportPaymentInfo	Allow importing of payment info
ImportSavedPasswords	Allow importing of saved passwords
ImportSearchEngine	Allow importing of search engine settings
ImportShortcuts	Allow importing of shortcuts
ImportStartupPageSettings	Allow importing of startup page settings
InAppSupportEnabled	In-app support Enabled
InPrivateModeAvailability	Configure InPrivate mode availability

POLICY NAME	CAPTION
InsecureFormsWarningsEnabled	Enable warnings for insecure forms
IntensiveWakeUpThrottlingEnabled	Control the IntensiveWakeUpThrottling feature
InternetExplorerIntegrationAlwaysUseOSCapture	Always use the OS capture engine to avoid issues with capturing Internet Explorer mode tabs
InternetExplorerIntegrationAlwaysWaitForUnload	Wait for Internet Explorer mode tabs to completely unload before ending the browser session
InternetExplorerIntegrationCloudNeutralSitesReporting	Configure reporting of potentially misconfigured neutral site URLs to the M365 Admin Center Site Lists app
InternetExplorerIntegrationCloudSiteList	Configure the Enterprise Mode Cloud Site List
InternetExplorerIntegrationCloudUserSitesReporting	Configure reporting of IE Mode user list entries to the M365 Admin Center Site Lists app
InternetExplorerIntegrationComplexNavDataTypes	Configure whether form data and HTTP headers will be sent when entering or exiting Internet Explorer mode
InternetExplorerIntegrationEnhancedHangDetection	Configure enhanced hang detection for Internet Explorer mode
InternetExplorerIntegrationLevel	Configure Internet Explorer integration
InternetExplorerIntegrationLocalFileAllowed	Allow launching of local files in Internet Explorer mode
InternetExplorerIntegrationLocalFileExtensionAllowList	Open local files in Internet Explorer mode file extension allow list
InternetExplorerIntegrationLocalFileShowContextMenu	Show context menu to open a file:// link in Internet Explorer mode
InternetExplorerIntegrationLocalMhtFileAllowed	Allow local MHTML files to open automatically in Internet Explorer mode
InternetExplorerIntegrationLocalSiteListExpirationDays	Specify the number of days that a site remains on the local IE mode site list
InternetExplorerIntegrationReloadInIEModeAllowed	Allow unconfigured sites to be reloaded in Internet Explorer mode
InternetExplorerIntegrationSiteList	Configure the Enterprise Mode Site List
InternetExplorerIntegrationSiteListRefreshInterval	Configure how frequently the Enterprise Mode Site List is refreshed
InternetExplorerIntegrationSiteRedirect	Specify how "in-page" navigations to unconfigured sites behave when started from Internet Explorer mode pages
InternetExplorerIntegrationTestingAllowed	Allow Internet Explorer mode testing (obsolete)

POLICY NAME	CAPTION
InternetExplorerIntegrationWindowOpenHeightAdjustment	Configure the pixel adjustment between window.open heights sourced from IE mode pages vs. Edge mode pages
InternetExplorerIntegrationWindowOpenWidthAdjustment	Configure the pixel adjustment between window.open widths sourced from IE mode pages vs. Edge mode pages
InternetExplorerModeEnableSavePageAs	Allow Save page as in Internet Explorer mode
InternetExplorerModeTabInEdgeModeAllowed	Allow sites configured for Internet Explorer mode to open in Microsoft Edge
InternetExplorerModeToolbarButtonEnabled	Show the Reload in Internet Explorer mode button in the toolbar
InternetExplorerZoomDisplay	Display zoom in IE Mode tabs with DPI Scale included like it is in Internet Explorer
IntranetRedirectBehavior	Intranet Redirection Behavior
IsolateOrigins	Enable site isolation for specific origins
LiveCaptionsAllowed	Live captions allowed
LocalBrowserDataShareEnabled	Enable Windows to search local Microsoft Edge browsing data
LocalProvidersEnabled	Allow suggestions from local providers
MAUEnabled	Always use Microsoft AutoUpdate as the updater for Microsoft Edge
MSAWebSiteSSOUsingThisProfileAllowed	Allow single sign-on for Microsoft personal sites using this profile
ManagedConfigurationPerOrigin	Sets managed configuration values for websites to specific origins
ManagedFavorites	Configure favorites
ManagedSearchEngines	Manage Search Engines
MathSolverEnabled	Let users snip a Math problem and get the solution with a step-by-step explanation in Microsoft Edge
MaxConnectionsPerProxy	Maximum number of concurrent connections to the proxy server
MediaRouterCastAllowAllIPs	Allow Google Cast to connect to Cast devices on all IP addresses
MetricsReportingEnabled	Enable usage and crash-related data reporting (obsolete)

POLICY NAME	CAPTION
MicrosoftEdgeInsiderPromotionEnabled	Microsoft Edge Insider Promotion Enabled
MicrosoftEditorProofingEnabled	Spell checking provided by Microsoft Editor
MicrosoftEditorSynonymsEnabled	Synonyms are provided when using Microsoft Editor spell checker
MicrosoftOfficeMenuEnabled	Allow users to access the Microsoft Office menu (deprecated)
NativeWindowOcclusionEnabled	Enable Native Window Occlusion (deprecated)
NavigationDelayForInitialSiteListDownloadTimeout	Set a timeout for delay of tab navigation for the Enterprise Mode Site List
NetworkPredictionOptions	Enable network prediction
NetworkServiceSandboxEnabled	Enable the network service sandbox
NonRemovableProfileEnabled	Configure whether a user always has a default profile automatically signed in with their work or school account
OriginAgentClusterDefaultEnabled	Origin-keyed agent clustering enabled by default
OutlookHubMenuEnabled	Allow users to access the Outlook menu (obsolete)
OverrideSecurityRestrictionsOnInsecureOrigin	Control where security restrictions on insecure origins apply
PDFSecureMode	Secure mode and Certificate-based Digital Signature validation in native PDF reader
PDFXFAEnabled	XFA support in native PDF reader enabled
PaymentMethodQueryEnabled	Allow websites to query for available payment methods
PersonalizationReportingEnabled	Allow personalization of ads, Microsoft Edge, search, news and other Microsoft services by sending browsing history, favorites and collections, usage and other browsing data to Microsoft
PinningWizardAllowed	Allow Pin to taskbar wizard
ProactiveAuthEnabled	Enable Proactive Authentication (obsolete)
PromotionalTabsEnabled	Enable full-tab promotional content
PromptForDownloadLocation	Ask where to save downloaded files
PromptOnMultipleMatchingCertificates	Prompt the user to select a certificate when multiple certificates match
QuicAllowed	Allow QUIC protocol

POLICY NAME	CAPTION
QuickSearchShowMiniMenu	Enables Microsoft Edge mini menu
QuickViewOfficeFilesEnabled	Manage QuickView Office files capability in Microsoft Edge
RedirectSitesFromInternetExplorerPreventBHOInstall	Prevent install of the BHO to redirect incompatible sites from Internet Explorer to Microsoft Edge
RedirectSitesFromInternetExplorerRedirectMode	Redirect incompatible sites from Internet Explorer to Microsoft Edge
RelatedMatchesCloudServiceEnabled	Configure Related Matches in Find on Page
RelaunchNotification	Notify a user that a browser restart is recommended or required for pending updates
RelaunchNotificationPeriod	Set the time period for update notifications
RelaunchWindow	Set the time interval for relaunch
RemoteDebuggingAllowed	Allow remote debugging
RendererAppContainerEnabled	Enable renderer in app container
RendererCodeIntegrityEnabled	Enable renderer code integrity
RequireOnlineRevocationChecksForLocalAnchors	Specify if online OCSP/CRL checks are required for local trust anchors
ResolveNavigationErrorsUseWebService	Enable resolution of navigation errors using a web service
RestrictSigninToPattern	Restrict which accounts can be used to sign in to Microsoft Edge
RoamingProfileLocation	Set the roaming profile directory
RoamingProfileSupportEnabled	Enable using roaming copies for Microsoft Edge profile data
RunAllFlashInAllowMode	Extend Adobe Flash content setting to all content (obsolete)
SSLErrorOverrideAllowed	Allow users to proceed from the HTTPS warning page
SSLErrorOverrideAllowedForOrigins	Allow users to proceed from the HTTPS warning page for specific origins
SSLVersionMin	Minimum TLS version enabled
SandboxExternalProtocolBlocked	Allow Microsoft Edge to block navigations to external protocols in a sandboxed iframe
SaveCookiesOnExit	Save cookies when Microsoft Edge closes

POLICY NAME	CAPTION
SavingBrowserHistoryDisabled	Disable saving browser history
ScreenCaptureAllowed	Allow or deny screen capture
ScrollToTextFragmentEnabled	Enable scrolling to text specified in URL fragments
SearchSuggestEnabled	Enable search suggestions
SecurityKeyPermitAttestation	Websites or domains that don't need permission to use direct Security Key attestation
SendIntranetToInternetExplorer	Send all intranet sites to Internet Explorer
SendSiteInfoToImproveServices	Send site information to improve Microsoft services (obsolete)
SensorsAllowedForUrls	Allow access to sensors on specific sites
SensorsBlockedForUrls	Block access to sensors on specific sites
SerialAskForUrls	Allow the Serial API on specific sites
SerialBlockedForUrls	Block the Serial API on specific sites
SetTimeoutWithout1MsClampEnabled	Control Javascript setTimeout() function minimum timeout (deprecated)
ShadowStackCrashRollbackBehavior	Configure ShadowStack crash rollback behavior (deprecated)
SharedArrayBufferUnrestrictedAccessAllowed	Specifies whether SharedArrayBuffers can be used in a non cross-origin-isolated context
SharedLinksEnabled	Show links shared from Microsoft 365 apps in History
ShowMicrosoftRewards	Show Microsoft Rewards experiences
ShowOfficeShortcutInFavoritesBar	Show Microsoft Office shortcut in favorites bar (deprecated)
ShowRecommendationsEnabled	Allow feature recommendations and browser assistance notifications from Microsoft Edge
SignedHTTPExchangeEnabled	Enable Signed HTTP Exchange (SXG) support
SitePerProcess	Enable site isolation for every site
SiteSafetyServicesEnabled	Allow users to configure Site safety services
SmartActionsBlockList	Block smart actions for a list of services
SpeechRecognitionEnabled	Configure Speech Recognition

POLICY NAME	CAPTION
SpellcheckEnabled	Enable spellcheck
SpellcheckLanguage	Enable specific spellcheck languages
SpellcheckLanguageBlocklist	Force disable spellcheck languages
StricterMixedContentTreatmentEnabled	Enable stricter treatment for mixed content (obsolete)
SuppressUnsupportedOSWarning	Suppress the unsupported OS warning
SyncDisabled	Disable synchronization of data using Microsoft sync services
SyncTypesListDisabled	Configure the list of types that are excluded from synchronization
TLS13HardeningForLocalAnchorsEnabled	Enable a TLS 1.3 security feature for local trust anchors (obsolete)
TLSCipherSuiteDenyList	Specify the TLS cipher suites to disable
TabFreezingEnabled	Allow freezing of background tabs (obsolete)
TargetBlankImpliesNoOpener	Do not set window.opener for links targeting _blank (obsolete)
TaskManagerEndProcessEnabled	Enable ending processes in the Browser task manager
TextPredictionEnabled	Text prediction enabled by default
TotalMemoryLimitMb	Set limit on megabytes of memory a single Microsoft Edge instance can use
TrackingPrevention	Block tracking of users' web-browsing activity
TranslateEnabled	Enable Translate
TravelAssistanceEnabled	Enable travel assistance (obsolete)
TripleDESEnabled	Enable 3DES cipher suites in TLS
U2fSecurityKeyApiEnabled	Allow using the deprecated U2F Security Key API (obsolete)
URLAllowlist	Define a list of allowed URLs
URLBlocklist	Block access to a list of URLs
UnthrottledNestedTimeoutEnabled	JavaScript setTimeout will not be clamped until a higher nesting threshold is set (deprecated)

POLICY NAME	CAPTION
UpdatePolicyOverride	Specifies how Microsoft Edge Update handles available updates from Microsoft Edge
UserAgentClientHintsEnabled	Enable the User-Agent Client Hints feature (obsolete)
UserAgentClientHintsGREASEUpdateEnabled	Control the User-Agent Client Hints GREASE Update feature
UserAgentReduction	Enable or disable the User-Agent Reduction
UserDataDir	Set the user data directory
UserDataSnapshotRetentionLimit	Limits the number of user data snapshots retained for use in case of emergency rollback
UserFeedbackAllowed	Allow user feedback
VerticalTabsAllowed	Configures availability of a vertical layout for tabs on the side of the browser
VideoCaptureAllowed	Allow or block video capture
VideoCaptureAllowedUrls	Sites that can access video capture devices without requesting permission
VisualSearchEnabled	Visual search enabled
WPADQuickCheckEnabled	Set WPAD optimization
WebAppInstallForceList	Configure list of force-installed Web Apps
WebCaptureEnabled	Enable web capture feature in Microsoft Edge
WebComponentsV0Enabled	Re-enable Web Components v0 API until M84 (obsolete)
WebDriverOverridesIncompatiblePolicies	Allow WebDriver to Override Incompatible Policies (obsolete)
WebRtcAllowLegacyTLSProtocols	Allow legacy TLS/DTLS downgrade in WebRTC (deprecated)
WebRtcLocalIpsAllowedUrls	Manage exposure of local IP addressess by WebRTC
WebRtcLocalhostIpHandling	Restrict exposure of local IP address by WebRTC
WebRtcRespectOsRoutingTableEnabled	Enable support for Windows OS routing table rules when making peer to peer connections via WebRTC
WebRtcUdpPortRange	Restrict the range of local UDP ports used by WebRTC
WebSQLAccess	Force WebSQL to be enabled
WebSQLInThirdPartyContextEnabled	Force WebSQL in third-party contexts to be re-enabled (obsolete)

POLICY NAME	CAPTION
WebSQLNonSecureContextEnabled	Force WebSQL in non-secure contexts to be enabled (deprecated)
WebSelectEnabled	Web Select Enabled
WebWidgetAllowed	Enable the Edge bar
WebWidgetIsEnabledOnStartup	Allow the Edge bar at Windows startup
WinHttpProxyResolverEnabled	Use Windows proxy resolver
WindowOcclusionEnabled	Enable Window Occlusion

Application Guard settings policies

Back to top

ApplicationGuardContainerProxy

Application Guard Container Proxy

Supported versions:

- On Windows since 84 or later

Description

Configures the proxy settings for Microsoft Edge Application Guard. If you enable this policy, Microsoft Edge Application Guard ignores other sources of proxy configurations.

If you don't configure this policy, Microsoft Edge Application Guard uses the proxy configuration of the host.

This policy does not affect the proxy configuration of Microsoft Edge outside of Application Guard (on the host).

The ProxyMode field lets you specify the proxy server used by Microsoft Edge Application Guard.

The ProxyPacUrl field is a URL to a proxy .pac file.

The ProxyServer field is a URL for the proxy server.

If you choose the 'direct' value as 'ProxyMode', all other fields are ignored.

If you choose the 'auto_detect' value as 'ProxyMode', all other fields are ignored.

If you choose the 'fixed_servers' value as 'ProxyMode', the 'ProxyServer' field is used.

If you choose the 'pac_script' value as 'ProxyMode', the 'ProxyPacUrl' field is used.

For more information about identifying Application Guard traffic via dual proxy, visit https://go.microsoft.com/fwlink/?linkid=2134653.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Dictionary

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ApplicationGuardContainerProxy
- GP name: Application Guard Container Proxy
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Application Guard settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ApplicationGuardContainerProxy
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ApplicationGuardContainerProxy = {
  "ProxyMode": "direct",
  "ProxyPacUrl": "https://internal.site/example.pac",
  "ProxyServer": "123.123.123.123:8080"
}
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\ApplicationGuardContainerProxy = {"ProxyMode": "direct", "ProxyPacUrl":
"https://internal.site/example.pac", "ProxyServer": "123.123.123.123:8080"}
```

Back to top

ApplicationGuardFavoritesSyncEnabled

Application Guard Favorites Sync Enabled

Supported versions:

- On Windows since 90 or later

Description

This policy allows Microsoft Edge computers/devices that have application guard enabled to sync favorites from the host to the container so the favorites match.

If ManagedFavorites are configured, those favorites will also be synced to the container.

If you enable this policy, editing favorites in the container is disabled. So, the add favorites and add favorites folder buttons will be blurred out in the UI of the container browser.

If you disable or don't configure this policy, favorites on the host will not be shared to the container.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ApplicationGuardFavoritesSyncEnabled
- GP name: Application Guard Favorites Sync Enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Application Guard settings
- GP path (Recommended): N/A

- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ApplicationGuardFavoritesSyncEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

ApplicationGuardPassiveModeEnabled

Ignore Application Guard site list configuration and browse Edge normally

Supported versions:

- On Windows since 94 or later

Description

Set whether Edge should ignore the Application Guard site list configuration for trusted and untrusted sites.

If you enable this policy, all navigations from Edge, including navigations to untrusted sites, will be accessed normally within Edge without redirecting to the Application Guard container. Note: this policy ONLY impacts Edge, so navigations from other browsers might get redirected to the Application Guard Container if you have the corresponding extensions enabled.

If you disable or don't configure this policy, Edge does not ignore the Application Guard site list. If users try to navigate to an untrusted site in the host, the site will open in the container.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ApplicationGuardPassiveModeEnabled
- GP name: Ignore Application Guard site list configuration and browse Edge normally
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Application Guard settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ApplicationGuardPassiveModeEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

ApplicationGuardTrafficIdentificationEnabled

Application Guard Traffic Identification

Supported versions:

- On Windows since 91 or later

Description

If you enable or don't configure this policy, Application Guard will add an extra HTTP header (X-MS-ApplicationGuard-Initiated) to all outbound HTTP requests made from the Application Guard container.

If you disable this policy, the extra header is not added to the traffic.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ApplicationGuardTrafficIdentificationEnabled
- GP name: Application Guard Traffic Identification
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Application Guard settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ApplicationGuardTrafficIdentificationEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

ApplicationGuardUploadBlockingEnabled

Prevents files from being uploaded while in Application Guard

Supported versions:

- On Windows since 96 or later

Description

Sets whether files can be uploaded while in Application Guard.

If you enable this policy, users will not be able to upload files in Application Guard.

If you disable or don't configure this policy, users will be able to upload files while in Application Guard.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ApplicationGuardUploadBlockingEnabled
- GP name: Prevents files from being uploaded while in Application Guard
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Application Guard settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ApplicationGuardUploadBlockingEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

Cast policies

Back to top

EnableMediaRouter

Enable Google Cast

Supported versions:

- On Windows and macOS since 77 or later

Description

Enable this policy to enable Google Cast. Users will be able to launch it from the app menu, page context menus, media controls on Cast-enabled websites, and (if shown) the Cast toolbar icon.

Disable this policy to disable Google Cast.

By default, Google Cast is enabled.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EnableMediaRouter
- GP name: Enable Google Cast
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Cast
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A

- Value Name: EnableMediaRouter
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: EnableMediaRouter
- Example value:

```
<true/>
```

Back to top

ShowCastIconInToolbar

Show the cast icon in the toolbar

Supported versions:

- On Windows and macOS since 77 or later

Description

Set this policy to true to show the Cast toolbar icon on the toolbar or the overflow menu. Users won't be able to remove it.

If you don't configure this policy or if you disable it, users can pin or remove the icon by using its contextual menu.

If you've also set the EnableMediaRouter policy to false, then this policy is ignored, and the toolbar icon isn't shown.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ShowCastIconInToolbar
- GP name: Show the cast icon in the toolbar
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Cast
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ShowCastIconInToolbar
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: ShowCastIconInToolbar
- Example value:

```
<false/>
```

Back to top

Content settings policies

Back to top

AutoSelectCertificateForUrls

Automatically select client certificates for these sites

Supported versions:

- On Windows and macOS since 77 or later

Description

Setting the policy lets you make a list of URL patterns that specify sites for which Microsoft Edge can automatically select a client certificate. The value is an array of stringified JSON dictionaries, each with the form { "pattern": "$URL_PATTERN", "filter" : $FILTER }, where $URL_PATTERN is a content setting pattern. $FILTER restricts the client certificates the browser automatically selects from. Independent of the filter, only certificates that match the server's certificate request are selected.

Examples for the usage of the $FILTER section:

- When $FILTER is set to { "ISSUER": { "CN": "$ISSUER_CN" } }, only client certificates issued by a certificate with the CommonName $ISSUER_CN are selected.
- When $FILTER contains both the "ISSUER" and the "SUBJECT" sections, only client certificates that satisfy both conditions are selected.
- When $FILTER contains a "SUBJECT" section with the "O" value, a certificate needs at least one organization matching the specified value to be selected.
- When $FILTER contains a "SUBJECT" section with a "OU" value, a certificate needs at least one organizational unit matching the specified value to be selected.
- When $FILTER is set to {}, the selection of client certificates is not additionally restricted. Note that filters provided by the web server still apply.

If you leave the policy unset, there's no autoselection for any site.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AutoSelectCertificateForUrls
- GP name: Automatically select client certificates for these sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A

- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\AutoSelectCertificateForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\AutoSelectCertificateForUrls\1 = "
{\"pattern\":\"https://www.contoso.com\",\"filter\":{\"ISSUER\":{\"CN\":\"certificate issuer name\", \"L\":
\"certificate issuer location\", \"O\": \"certificate issuer org\", \"OU\": \"certificate issuer org
unit\"}, \"SUBJECT\":{\"CN\":\"certificate subject name\", \"L\": \"certificate subject location\", \"O\":
\"certificate subject org\", \"OU\": \"certificate subject org unit\"}}}"
```

Mac information and settings

- Preference Key Name: AutoSelectCertificateForUrls
- Example value:

```
<array>
  <string>{"pattern":"https://www.contoso.com","filter":{"ISSUER":{"CN":"certificate issuer name", "L":
"certificate issuer location", "O": "certificate issuer org", "OU": "certificate issuer org unit"},
"SUBJECT":{"CN":"certificate subject name", "L": "certificate subject location", "O": "certificate subject
org", "OU": "certificate subject org unit"}}}</string>
</array>
```

Back to top

CookiesAllowedForUrls

Allow cookies on specific sites

Supported versions:

- On Windows and macOS since 77 or later

Description

Define a list of sites, based on URL patterns, that are allowed to set cookies.

If you don't configure this policy, the global default value from the DefaultCookiesSetting policy (if set) or the user's personal configuration is used for all sites.

See the CookiesBlockedForUrls and CookiesSessionOnlyForUrls policies for more information.

Note there cannot be conflicting URL patterns set between these three policies:

- CookiesBlockedForUrls
- CookiesAllowedForUrls
- CookiesSessionOnlyForUrls

For detailed information about valid url patterns, see https://go.microsoft.com/fwlink/?linkid=2095322. * is not an accepted value for this policy.

To allow third-party cookies to be set, specify a pair of URL patterns delimited by a comma. The first value in the pair specifies the third-party site that should be allowed to use cookies. The second value in the pair specifies the top-level site that the first value should be applied on. The first value in the pair supports * but the second value does not.

To exclude cookies from being deleted on exit, configure the SaveCookiesOnExit policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: CookiesAllowedForUrls
- GP name: Allow cookies on specific sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\CookiesAllowedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\CookiesAllowedForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\CookiesAllowedForUrls\2 = "[*.]contoso.edu"
SOFTWARE\Policies\Microsoft\Edge\CookiesAllowedForUrls\3 = "https://loaded-as-third-
party.fabrikam.com,https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\CookiesAllowedForUrls\4 = "*,https://www.contoso.com"
```

Mac information and settings

- Preference Key Name: CookiesAllowedForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
  <string>https://loaded-as-third-party.fabrikam.com,https://www.contoso.com</string>
  <string>*,https://www.contoso.com</string>
</array>
```

Back to top

CookiesBlockedForUrls

Block cookies on specific sites

Supported versions:

- On Windows and macOS since 77 or later

Description

Define a list of sites, based on URL patterns, that can't set cookies.

If you don't configure this policy, the global default value from the DefaultCookiesSetting policy (if set) or the user's personal configuration is used for all sites.

See the CookiesAllowedForUrls and CookiesSessionOnlyForUrls policies for more information.

Note there cannot be conflicting URL patterns set between these three policies:

- CookiesBlockedForUrls
- CookiesAllowedForUrls
- CookiesSessionOnlyForUrls

For detailed information on valid url patterns, please see https://go.microsoft.com/fwlink/?linkid=2095322. * is not an accepted value for this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: CookiesBlockedForUrls
- GP name: Block cookies on specific sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\CookiesBlockedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\CookiesBlockedForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\CookiesBlockedForUrls\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: CookiesBlockedForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

CookiesSessionOnlyForUrls

Limit cookies from specific websites to the current session

Supported versions:

- On Windows and macOS since 77 or later

Description

Cookies created by websites that match a URL pattern you define are deleted when the session ends (when the

window closes).

Cookies created by websites that don't match the pattern are controlled by the DefaultCookiesSetting policy (if set) or by the user's personal configuration. This is also the default behavior if you don't configure this policy.

You can also use the CookiesAllowedForUrls and CookiesBlockedForUrls policies to control which websites can create cookies.

Note there cannot be conflicting URL patterns set between these three policies:

- CookiesBlockedForUrls
- CookiesAllowedForUrls
- CookiesSessionOnlyForUrls

For detailed information on valid url patterns, please see https://go.microsoft.com/fwlink/?linkid=2095322. * is not an accepted value for this policy.

If you set the RestoreOnStartup policy to restore URLs from previous sessions, this policy is ignored, and cookies are stored permanently for those sites.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: CookiesSessionOnlyForUrls
- GP name: Limit cookies from specific websites to the current session
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\CookiesSessionOnlyForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\CookiesSessionOnlyForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\CookiesSessionOnlyForUrls\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: CookiesSessionOnlyForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

DefaultCookiesSetting

Configure cookies

Supported versions:

- On Windows and macOS since 77 or later

Description

Control whether websites can create cookies on the user's device. This policy is all or nothing - you can let all websites create cookies, or no websites create cookies. You can't use this policy to enable cookies from specific websites.

Set the policy to 'SessionOnly' to clear cookies when the session closes.

If you don't configure this policy, the default 'AllowCookies' is used, and users can change this setting in Microsoft Edge Settings. (If you don't want users to be able to change this setting, set the policy.)

Policy options mapping:

- AllowCookies (1) = Let all sites create cookies
- BlockCookies (2) = Don't let any site create cookies
- SessionOnly (4) = Keep cookies for the duration of the session, except ones listed in SaveCookiesOnExit

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultCookiesSetting
- GP name: Configure cookies
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefaultCookiesSetting
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: DefaultCookiesSetting
- Example value:

```
<integer>1</integer>
```

Back to top

DefaultFileSystemReadGuardSetting

Control use of the File System API for reading

Supported versions:

- On Windows and macOS since 86 or later

Description

If you set this policy to 3, websites can ask for read access to the host operating system's filesystem using the File System API. If you set this policy to 2, access is denied.

If you don't set this policy, websites can ask for access. Users can change this setting.

Policy options mapping:

- BlockFileSystemRead (2) = Don't allow any site to request read access to files and directories via the File System API
- AskFileSystemRead (3) = Allow sites to ask the user to grant read access to files and directories via the File System API

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultFileSystemReadGuardSetting
- GP name: Control use of the File System API for reading
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefaultFileSystemReadGuardSetting
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: DefaultFileSystemReadGuardSetting
- Example value:

```
<integer>2</integer>
```

Back to top

DefaultFileSystemWriteGuardSetting

Control use of the File System API for writing

Supported versions:

- On Windows and macOS since 86 or later

Description

If you set this policy to 3, websites can ask for write access to the host operating system's filesystem using the File System API. If you set this policy to 2, access is denied.

If you don't set this policy, websites can ask for access. Users can change this setting.

Policy options mapping:

- BlockFileSystemWrite (2) = Don't allow any site to request write access to files and directories
- AskFileSystemWrite (3) = Allow sites to ask the user to grant write access to files and directories

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultFileSystemWriteGuardSetting
- GP name: Control use of the File System API for writing
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefaultFileSystemWriteGuardSetting
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: DefaultFileSystemWriteGuardSetting
- Example value:

```
<integer>2</integer>
```

Back to top

DefaultGeolocationSetting

Default geolocation setting

Supported versions:

- On Windows and macOS since 77 or later

Description

Set whether websites can track users' physical locations. You can allow tracking by default ('AllowGeolocation'), deny it by default ('BlockGeolocation'), or ask the user each time a website requests their location ('AskGeolocation').

If you don't configure this policy, 'AskGeolocation' is used and the user can change it.

Policy options mapping:

- AllowGeolocation (1) = Allow sites to track users' physical location
- BlockGeolocation (2) = Don't allow any site to track users' physical location
- AskGeolocation (3) = Ask whenever a site wants to track users' physical location

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultGeolocationSetting
- GP name: Default geolocation setting
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefaultGeolocationSetting
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: DefaultGeolocationSetting
- Example value:

```
<integer>1</integer>
```

Back to top

DefaultImagesSetting

Default images setting

Supported versions:

- On Windows and macOS since 77 or later

Description

Set whether websites can display images. You can allow images on all sites ('AllowImages') or block them on all sites ('BlockImages').

If you don't configure this policy, images are allowed by default, and the user can change this setting.

Policy options mapping:

- AllowImages (1) = Allow all sites to show all images
- BlockImages (2) = Don't allow any site to show images

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultImagesSetting
- GP name: Default images setting
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefaultImagesSetting
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: DefaultImagesSetting
- Example value:

```
<integer>1</integer>
```

Back to top

DefaultInsecureContentSetting

Control use of insecure content exceptions

Supported versions:

- On Windows and macOS since 80 or later

Description

Allows you to set whether users can add exceptions to allow mixed content for specific sites.

This policy can be overridden for specific URL patterns using the InsecureContentAllowedForUrls and InsecureContentBlockedForUrls policies.

If this policy isn't set, users will be allowed to add exceptions to allow blockable mixed content and disable autoupgrades for optionally blockable mixed content.

Policy options mapping:

- BlockInsecureContent (2) = Do not allow any site to load mixed content
- AllowExceptionsInsecureContent (3) = Allow users to add exceptions to allow mixed content

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultInsecureContentSetting
- GP name: Control use of insecure content exceptions
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefaultInsecureContentSetting
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: DefaultInsecureContentSetting
- Example value:

```
<integer>2</integer>
```

Back to top

DefaultJavaScriptJitSetting

Control use of JavaScript JIT

Supported versions:

- On Windows and macOS since 93 or later

Description

Allows you to set whether Microsoft Edge will run the v8 JavaScript engine with JIT (Just In Time) compiler enabled or not.

Disabling the JavaScript JIT will mean that Microsoft Edge may render web content more slowly, and may also disable parts of JavaScript including WebAssembly. Disabling the JavaScript JIT may allow Microsoft Edge to render web content in a more secure configuration.

This policy can be overridden for specific URL patterns using the JavaScriptJitAllowedForSites and JavaScriptJitBlockedForSites policies.

If you don't configure this policy, JavaScript JIT is enabled.

Policy options mapping:

- AllowJavaScriptJit (1) = Allow any site to run JavaScript JIT
- BlockJavaScriptJit (2) = Do not allow any site to run JavaScript JIT

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultJavaScriptJitSetting
- GP name: Control use of JavaScript JIT
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefaultJavaScriptJitSetting
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: DefaultJavaScriptJitSetting
- Example value:

```
<integer>1</integer>
```

Back to top

DefaultJavaScriptSetting

Default JavaScript setting

Supported versions:

- On Windows and macOS since 77 or later

Description

Set whether websites can run JavaScript. You can allow it for all sites ('AllowJavaScript') or block it for all sites ('BlockJavaScript').

If you don't configure this policy, all sites can run JavaScript by default, and the user can change this setting.

Policy options mapping:

- AllowJavaScript (1) = Allow all sites to run JavaScript
- BlockJavaScript (2) = Don't allow any site to run JavaScript

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultJavaScriptSetting
- GP name: Default JavaScript setting
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefaultJavaScriptSetting
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: DefaultJavaScriptSetting
- Example value:

```
<integer>1</integer>
```

Back to top

DefaultNotificationsSetting

Default notification setting

Supported versions:

- On Windows and macOS since 77 or later

Description

Set whether websites can display desktop notifications. You can allow them by default ('AllowNotifications'),

deny them by default ('BlockNotifications'), or have the user be asked each time a website wants to show a notification ('AskNotifications').

If you don't configure this policy, notifications are allowed by default, and the user can change this setting.

Policy options mapping:

- AllowNotifications (1) = Allow sites to show desktop notifications
- BlockNotifications (2) = Don't allow any site to show desktop notifications
- AskNotifications (3) = Ask every time a site wants to show desktop notifications

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultNotificationsSetting
- GP name: Default notification setting
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefaultNotificationsSetting
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: DefaultNotificationsSetting
- Example value:

```
<integer>2</integer>
```

Back to top

DefaultPluginsSetting

Default Adobe Flash setting (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 87.

Supported versions:

- On Windows and macOS since 77, until 87

Description

This policy doesn't work because Flash is no longer supported by Microsoft Edge.

PluginsAllowedForUrls and PluginsBlockedForUrls are checked first, then this policy. The options are 'ClickToPlay' and 'BlockPlugins'. If you set this policy to 'BlockPlugins', this plugin is denied for all websites. 'ClickToPlay' lets the Flash plugin run, but users click the placeholder to start it.

If you don't configure this policy, the user can change this setting manually.

Note: Automatic playback is only for domains explicitly listed in the PluginsAllowedForUrls policy. To turn automatic playback on for all sites, add http://* and https://* to the allowed list of URLs.

Policy options mapping:

- BlockPlugins (2) = Block the Adobe Flash plugin
- ClickToPlay (3) = Click to play

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultPluginsSetting
- GP name: Default Adobe Flash setting (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefaultPluginsSetting
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: DefaultPluginsSetting
- Example value:

```
<integer>2</integer>
```

Back to top

DefaultPopupsSetting

Default pop-up window setting

Supported versions:

- On Windows and macOS since 77 or later

Description

Set whether websites can show pop-up windows. You can allow them on all websites ('AllowPopups') or block them on all sites ('BlockPopups').

If you don't configure this policy, pop-up windows are blocked by default, and users can change this setting.

Policy options mapping:

- AllowPopups (1) = Allow all sites to show pop-ups
- BlockPopups (2) = Do not allow any site to show popups

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultPopupsSetting
- GP name: Default pop-up window setting
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefaultPopupsSetting
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: DefaultPopupsSetting
- Example value:

```
<integer>1</integer>
```

Back to top

DefaultWebBluetoothGuardSetting

Control use of the Web Bluetooth API

Supported versions:

- On Windows and macOS since 77 or later

Description

Control whether websites can access nearby Bluetooth devices. You can completely block access or require the

site to ask the user each time it wants to access a Bluetooth device.

If you don't configure this policy, the default value ('AskWebBluetooth', meaning users are asked each time) is used and users can change it.

Policy options mapping:

- BlockWebBluetooth (2) = Do not allow any site to request access to Bluetooth devices via the Web Bluetooth API
- AskWebBluetooth (3) = Allow sites to ask the user to grant access to a nearby Bluetooth device

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultWebBluetoothGuardSetting
- GP name: Control use of the Web Bluetooth API
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefaultWebBluetoothGuardSetting
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: DefaultWebBluetoothGuardSetting
- Example value:

```
<integer>2</integer>
```

Back to top

DefaultWebHidGuardSetting

Control use of the WebHID API

Supported versions:

- On Windows and macOS since 100 or later

Description

Setting the policy to 3 lets websites ask for access to HID devices. Setting the policy to 2 denies access to HID devices.

Leaving it unset lets websites ask for access, but users can change this setting.

This policy can be overridden for specific url patterns using the WebHidAskForUrls and WebHidBlockedForUrls policies.

Policy options mapping:

- BlockWebHid (2) = Do not allow any site to request access to HID devices via the WebHID API
- AskWebHid (3) = Allow sites to ask the user to grant access to a HID device

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultWebHidGuardSetting
- GP name: Control use of the WebHID API
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefaultWebHidGuardSetting
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: DefaultWebHidGuardSetting
- Example value:

```
<integer>2</integer>
```

Back to top

DefaultWebUsbGuardSetting

Control use of the WebUSB API

Supported versions:

- On Windows and macOS since 77 or later

Description

Set whether websites can access connected USB devices. You can completely block access or ask the user each time a website wants to get access to connected USB devices.

You can override this policy for specific URL patterns by using the WebUsbAskForUrls and

WebUsbBlockedForUrls policies.

If you don't configure this policy, sites can ask users whether they can access the connected USB devices ('AskWebUsb') by default, and users can change this setting.

Policy options mapping:

- BlockWebUsb (2) = Do not allow any site to request access to USB devices via the WebUSB API
- AskWebUsb (3) = Allow sites to ask the user to grant access to a connected USB device

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultWebUsbGuardSetting
- GP name: Control use of the WebUSB API
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefaultWebUsbGuardSetting
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: DefaultWebUsbGuardSetting
- Example value:

```
<integer>2</integer>
```

Back to top

FileSystemReadAskForUrls

Allow read access via the File System API on these sites

Supported versions:

- On Windows and macOS since 86 or later

Description

Setting the policy lets you list the URL patterns that specify which sites can ask users to grant them read access to files or directories in the host operating system's file system via the File System API.

Leaving the policy unset means DefaultFileSystemReadGuardSetting applies for all sites, if it's set. If not, users'

personal settings apply.

URL patterns can't conflict with FileSystemReadBlockedForUrls. Neither policy takes precedence if a URL matches with both.

For detailed information about valid url patterns, see https://go.microsoft.com/fwlink/?linkid=2095322. * is not an accepted value for this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: FileSystemReadAskForUrls
- GP name: Allow read access via the File System API on these sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\FileSystemReadAskForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\FileSystemReadAskForUrls\1 = "https://www.example.com"
SOFTWARE\Policies\Microsoft\Edge\FileSystemReadAskForUrls\2 = "[*.]example.edu"
```

Mac information and settings

- Preference Key Name: FileSystemReadAskForUrls
- Example value:

```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

FileSystemReadBlockedForUrls

Block read access via the File System API on these sites

Supported versions:

- On Windows and macOS since 86 or later

Description

If you set this policy, you can list the URL patterns that specify which sites can't ask users to grant them read access to files or directories in the host operating system's file system via the File System API.

If you don't set this policy, DefaultFileSystemReadGuardSetting applies for all sites, if it's set. If not, users'

personal settings apply.

URL patterns can't conflict with FileSystemReadAskForUrls. Neither policy takes precedence if a URL matches with both.

For detailed information about valid url patterns, see https://go.microsoft.com/fwlink/?linkid=2095322. * is not an accepted value for this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: FileSystemReadBlockedForUrls
- GP name: Block read access via the File System API on these sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\FileSystemReadBlockedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\FileSystemReadBlockedForUrls\1 = "https://www.example.com"
SOFTWARE\Policies\Microsoft\Edge\FileSystemReadBlockedForUrls\2 = "[*.]example.edu"
```

Mac information and settings

- Preference Key Name: FileSystemReadBlockedForUrls
- Example value:

```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

FileSystemWriteAskForUrls

Allow write access to files and directories on these sites

Supported versions:

- On Windows and macOS since 86 or later

Description

If you set this policy, you can list the URL patterns that specify which sites can ask users to grant them write access to files or directories in the host operating system's file system.

If you don't set this policy, DefaultFileSystemWriteGuardSetting applies for all sites, if it's set. If not, users'

personal settings apply.

URL patterns can't conflict with FileSystemWriteBlockedForUrls. Neither policy takes precedence if a URL matches with both.

For detailed information about valid url patterns, see https://go.microsoft.com/fwlink/?linkid=2095322. * is not an accepted value for this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: FileSystemWriteAskForUrls
- GP name: Allow write access to files and directories on these sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\FileSystemWriteAskForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\FileSystemWriteAskForUrls\1 = "https://www.example.com"
SOFTWARE\Policies\Microsoft\Edge\FileSystemWriteAskForUrls\2 = "[*.]example.edu"
```

Mac information and settings

- Preference Key Name: FileSystemWriteAskForUrls
- Example value:

```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

FileSystemWriteBlockedForUrls

Block write access to files and directories on these sites

Supported versions:

- On Windows and macOS since 86 or later

Description

If you set this policy, you can list the URL patterns that specify which sites can't ask users to grant them write access to files or directories in the host operating system's file system.

If you don't set this policy, DefaultFileSystemWriteGuardSetting applies for all sites, if it's set. If not, users'

personal settings apply.

URL patterns can't conflict with FileSystemWriteAskForUrls. Neither policy takes precedence if a URL matches with both.

For detailed information about valid url patterns, see https://go.microsoft.com/fwlink/?linkid=2095322. * is not an accepted value for this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: FileSystemWriteBlockedForUrls
- GP name: Block write access to files and directories on these sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\FileSystemWriteBlockedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\FileSystemWriteBlockedForUrls\1 = "https://www.example.com"
SOFTWARE\Policies\Microsoft\Edge\FileSystemWriteBlockedForUrls\2 = "[*.]example.edu"
```

Mac information and settings

- Preference Key Name: FileSystemWriteBlockedForUrls
- Example value:

```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

ImagesAllowedForUrls

Allow images on these sites

Supported versions:

- On Windows and macOS since 77 or later

Description

Define a list of sites, based on URL patterns, that can display images.

If you don't configure this policy, the global default value is used for all sites either from the DefaultImagesSetting policy (if set) or the user's personal configuration.

For detailed information about valid url patterns, see https://go.microsoft.com/fwlink/?linkid=2095322. * is not an accepted value for this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ImagesAllowedForUrls
- GP name: Allow images on these sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\ImagesAllowedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ImagesAllowedForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\ImagesAllowedForUrls\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: ImagesAllowedForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

ImagesBlockedForUrls

Block images on specific sites

Supported versions:

- On Windows and macOS since 77 or later

Description

Define a list of sites, based on URL patterns, that aren't allowed to display images.

If you don't configure this policy, the global default value from the DefaultImagesSetting policy (if set) or the user's personal configuration is used for all sites.

For detailed information about valid url patterns, see https://go.microsoft.com/fwlink/?linkid=2095322. * is not an accepted value for this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ImagesBlockedForUrls
- GP name: Block images on specific sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\ImagesBlockedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ImagesBlockedForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\ImagesBlockedForUrls\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: ImagesBlockedForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

InsecureContentAllowedForUrls

Allow insecure content on specified sites

Supported versions:

- On Windows and macOS since 80 or later

Description

Create a list of URL patterns to specify sites that can display or, as of version 94, download insecure mixed content (that is, HTTP content on HTTPS sites).

If you don't configure this policy, blockable mixed content will be blocked and optionally blockable mixed content will be upgraded. However, users will be allowed to set exceptions to allow insecure mixed content for specific sites.

For detailed information about valid url patterns, see https://go.microsoft.com/fwlink/?linkid=2095322. * is not an accepted value for this policy.

Supported features:

- Can be mandatory: Yes

- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InsecureContentAllowedForUrls
- GP name: Allow insecure content on specified sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\InsecureContentAllowedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\InsecureContentAllowedForUrls\1 = "https://www.example.com"
SOFTWARE\Policies\Microsoft\Edge\InsecureContentAllowedForUrls\2 = "[*.]example.edu"
```

Mac information and settings

- Preference Key Name: InsecureContentAllowedForUrls
- Example value:

```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

InsecureContentBlockedForUrls

Block insecure content on specified sites

Supported versions:

- On Windows and macOS since 80 or later

Description

Create a list of URL patterns to specify sites that aren't allowed to display blockable (i.e. active) mixed content (that is, HTTP content on HTTPS sites) and for which optionally blockable mixed content upgrades will be disabled.

If you don't configure this policy, blockable mixed content will be blocked and optionally blockable mixed content will be upgraded. However, users will be allowed to set exceptions to allow insecure mixed content for specific sites.

For detailed information about valid url patterns, see https://go.microsoft.com/fwlink/?linkid=2095322. * is not an accepted value for this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No

- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InsecureContentBlockedForUrls
- GP name: Block insecure content on specified sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\InsecureContentBlockedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\InsecureContentBlockedForUrls\1 = "https://www.example.com"
SOFTWARE\Policies\Microsoft\Edge\InsecureContentBlockedForUrls\2 = "[*.]example.edu"
```

Mac information and settings

- Preference Key Name: InsecureContentBlockedForUrls
- Example value:

```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

IntranetFileLinksEnabled

Allow intranet zone file URL links from Microsoft Edge to open in Windows File Explorer

Supported versions:

- On Windows since 95 or later

Description

This setting allows file URL links to intranet zone files from intranet zone HTTPS websites to open Windows File Explorer for that file or directory.

If you enable this policy, intranet zone file URL links originating from intranet zone HTTPS pages will open Windows File Explorer to the parent directory of the file and select the file. Intranet zone directory URL links originating from intranet zone HTTPS pages will open Windows File Explorer to the directory with no items in the directory selected.

If you disable or don't configure this policy, file URL links will not open.

Microsoft Edge uses the definition of intranet zone as configured for Internet Explorer. Note that https://localhost/ is specifically blocked as an exception of allowed intranet zone host, while loopback addresses (127.0.0.*, [::1]) are considered internet zone by default.

Users may opt out of prompts on a per-protocol/per-site basis unless the

ExternalProtocolDialogShowAlwaysOpenCheckbox policy is disabled.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: IntranetFileLinksEnabled
- GP name: Allow intranet zone file URL links from Microsoft Edge to open in Windows File Explorer
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: IntranetFileLinksEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

JavaScriptAllowedForUrls

Allow JavaScript on specific sites

Supported versions:

- On Windows and macOS since 77 or later

Description

Define a list of sites, based on URL patterns, that are allowed to run JavaScript.

If you don't configure this policy, DefaultJavaScriptSetting applies for all sites, if it's set. If not, the user's personal setting applies.

For detailed information on valid url patterns, please see https://go.microsoft.com/fwlink/?linkid=2095322. * is not an accepted value for this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: JavaScriptAllowedForUrls
- GP name: Allow JavaScript on specific sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings

- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\JavaScriptAllowedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\JavaScriptAllowedForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\JavaScriptAllowedForUrls\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: JavaScriptAllowedForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

JavaScriptBlockedForUrls

Block JavaScript on specific sites

Supported versions:

- On Windows and macOS since 77 or later

Description

Define a list of sites, based on URL patterns, that aren't allowed to run JavaScript.

If you don't configure this policy, DefaultJavaScriptSetting applies for all sites, if it's set. If not, the user's personal setting applies.

For detailed information on valid url patterns, please see https://go.microsoft.com/fwlink/?linkid=2095322. * is not an accepted value for this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: JavaScriptBlockedForUrls
- GP name: Block JavaScript on specific sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\JavaScriptBlockedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\JavaScriptBlockedForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\JavaScriptBlockedForUrls\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: JavaScriptBlockedForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

JavaScriptJitAllowedForSites

Allow JavaScript to use JIT on these sites

Supported versions:

- On Windows and macOS since 93 or later

Description

Allows you to set a list of site url patterns that specify sites which are allowed to run JavaScript with JIT (Just In Time) compiler enabled.

For detailed information on valid site url patterns, please see https://go.microsoft.com/fwlink/?linkid=2095322. * is not an accepted value for this policy.

JavaScript JIT policy exceptions will only be enforced at a site granularity (eTLD+1). A policy set for only subdomain.contoso.com will not correctly apply to contoso.com or subdomain.contoso.com since they both resolve to the same eTLD+1 (contoso.com) for which there is no policy. In this case, policy must be set on contoso.com to apply correctly for both contoso.com and subdomain.contoso.com.

This policy applies on a frame-by-frame basis and not based on top level origin url alone, so e.g. if contoso.com is listed in the JavaScriptJitAllowedForSites policy but contoso.com loads a frame containing fabrikam.com then contoso.com will have JavaScript JIT enabled, but fabrikam.com will use the policy from DefaultJavaScriptJitSetting, if set, or default to JavaScript JIT enabled.

If you don't configure this policy for a site then the policy from DefaultJavaScriptJitSetting applies to the site, if set, otherwise Javascript JIT is enabled for the site.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: JavaScriptJitAllowedForSites
- GP name: Allow JavaScript to use JIT on these sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\JavaScriptJitAllowedForSites
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\JavaScriptJitAllowedForSites\1 = "[*.]example.edu"
```

Mac information and settings

- Preference Key Name: JavaScriptJitAllowedForSites
- Example value:

```
<array>
  <string>[*.]example.edu</string>
</array>
```

Back to top

JavaScriptJitBlockedForSites

Block JavaScript from using JIT on these sites

Supported versions:

- On Windows and macOS since 93 or later

Description

Allows you to set a list of site url patterns that specify sites which are not allowed to run JavaScript JIT (Just In Time) compiler enabled.

Disabling the JavaScript JIT will mean that Microsoft Edge may render web content more slowly, and may also disable parts of JavaScript including WebAssembly. Disabling the JavaScript JIT may allow Microsoft Edge to render web content in a more secure configuration.

For detailed information on valid url patterns, please see https://go.microsoft.com/fwlink/?linkid=2095322. * is not an accepted value for this policy.

JavaScript JIT policy exceptions will only be enforced at a site granularity (eTLD+1). A policy set for only subdomain.contoso.com will not correctly apply to contoso.com or subdomain.contoso.com since they both resolve to the same eTLD+1 (contoso.com) for which there is no policy. In this case, policy must be set on contoso.com to apply correctly for both contoso.com and subdomain.contoso.com.

This policy applies on a frame-by-frame basis and not based on top level origin url alone, so e.g. if contoso.com is listed in the JavaScriptJitBlockedForSites policy but contoso.com loads a frame containing fabrikam.com then contoso.com will have JavaScript JIT disabled, but fabrikam.com will use the policy from DefaultJavaScriptJitSetting, if set, or default to JavaScript JIT enabled.

If you don't configure this policy for a site then the policy from DefaultJavaScriptJitSetting applies to the site, if set, otherwise JavaScript JIT is enabled for the site.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: JavaScriptJitBlockedForSites
- GP name: Block JavaScript from using JIT on these sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\JavaScriptJitBlockedForSites
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\JavaScriptJitBlockedForSites\1 = "[*.]example.edu"
```

Mac information and settings

- Preference Key Name: JavaScriptJitBlockedForSites
- Example value:

```
<array>
  <string>[*.]example.edu</string>
</array>
```

Back to top

LegacySameSiteCookieBehaviorEnabled

Enable default legacy SameSite cookie behavior setting (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 94.

Supported versions:

- On Windows and macOS since 80, until 94

Description

This policy doesn't work because it was only intended to serve only as a short-term mechanism to give enterprises more time to update their environments if they were found to be incompatible with the SameSite behavior change.

If you still require legacy cookie behavior, please use LegacySameSiteCookieBehaviorEnabledForDomainList to configure behavior on a per-domain basis.

Lets you revert all cookies to legacy SameSite behavior. Reverting to legacy behavior causes cookies that don't specify a SameSite attribute to be treated as if they were "SameSite=None", removes the requirement for "SameSite=None" cookies to carry the "Secure" attribute, and skips the scheme comparison when evaluating if

two sites are same-site.

If you don't set this policy, the default SameSite behavior for cookies will depend on other configuration sources for the SameSite-by-default feature, the Cookies-without-SameSite-must-be-secure feature, and the Schemeful Same-Site feature. These features can also be configured by a field trial or the same-site-by-default-cookies flag, the cookies-without-same-site-must-be-secure flag, or the schemeful-same-site flag in edge://flags.

Policy options mapping:

- DefaultToLegacySameSiteCookieBehavior (1) = Revert to legacy SameSite behavior for cookies on all sites
- DefaultToSameSiteByDefaultCookieBehavior (2) = Use SameSite-by-default behavior for cookies on all sites

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: LegacySameSiteCookieBehaviorEnabled
- GP name: Enable default legacy SameSite cookie behavior setting (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: LegacySameSiteCookieBehaviorEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: LegacySameSiteCookieBehaviorEnabled
- Example value:

```
<integer>1</integer>
```

Back to top

LegacySameSiteCookieBehaviorEnabledForDomainList

Revert to legacy SameSite behavior for cookies on specified sites

Supported versions:

- On Windows and macOS since 80 or later

Description

Cookies set for domains match specified patterns will revert to legacy SameSite behavior.

Reverting to legacy behavior causes cookies that don't specify a SameSite attribute to be treated as if they were "SameSite=None", removes the requirement for "SameSite=None" cookies to carry the "Secure" attribute, and skips the scheme comparison when evaluating if two sites are same-site.

If you don't set this policy, the global default value will be used. The global default will also be used for cookies on domains not covered by the patterns you specify.

The global default value can be configured using the LegacySameSiteCookieBehaviorEnabled policy. If LegacySameSiteCookieBehaviorEnabled is unset, the global default value falls back to other configuration sources.

For detailed information about valid URL patterns, see https://go.microsoft.com/fwlink/?linkid=2095322.

Note that patterns you list in this policy are treated as domains, not URLs, so you should not specify a scheme or port.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: LegacySameSiteCookieBehaviorEnabledForDomainList
- GP name: Revert to legacy SameSite behavior for cookies on specified sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\LegacySameSiteCookieBehaviorEnabledForDomainList
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\LegacySameSiteCookieBehaviorEnabledForDomainList\1 = "www.example.com"
SOFTWARE\Policies\Microsoft\Edge\LegacySameSiteCookieBehaviorEnabledForDomainList\2 = "[*.]example.edu"
```

Mac information and settings

- Preference Key Name: LegacySameSiteCookieBehaviorEnabledForDomainList
- Example value:

```
<array>
  <string>www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

NotificationsAllowedForUrls

Allow notifications on specific sites

Supported versions:

- On Windows and macOS since 77 or later

Description

Allows you to create a list of url patterns to specify sites that are allowed to display notifications.

If you don't set this policy, the global default value will be used for all sites. This default value will be from the DefaultNotificationsSetting policy if it's set, or from the user's personal configuration. For detailed information on valid url patterns, see https://go.microsoft.com/fwlink/?linkid=2095322.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NotificationsAllowedForUrls
- GP name: Allow notifications on specific sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\NotificationsAllowedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\NotificationsAllowedForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\NotificationsAllowedForUrls\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: NotificationsAllowedForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

NotificationsBlockedForUrls

Block notifications on specific sites

Supported versions:

- On Windows and macOS since 77 or later

Description

Allows you to create a list of url patterns to specify sites that are not allowed to display notifications.

If you don't set this policy, the global default value will be used for all sites. This default value will be from the DefaultNotificationsSetting policy if it's set, or from the user's personal configuration. For detailed information on valid url patterns, see https://go.microsoft.com/fwlink/?linkid=2095322.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NotificationsBlockedForUrls
- GP name: Block notifications on specific sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\NotificationsBlockedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\NotificationsBlockedForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\NotificationsBlockedForUrls\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: NotificationsBlockedForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

PluginsAllowedForUrls

Allow the Adobe Flash plug-in on specific sites (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 87.

Supported versions:

- On Windows and macOS since 77, until 87

Description

This policy doesn't work because Flash is no longer supported by Microsoft Edge.

Define a list of sites, based on URL patterns, that can run the Adobe Flash plug-in.

If you don't configure this policy, the global default value from the DefaultPluginsSetting policy (if set) or the user's personal configuration is used for all sites.

For detailed information on valid url patterns, see https://go.microsoft.com/fwlink/?linkid=2095322. However, starting in M85, patterns with '*' and '[*.]' wildcards in the host are no longer supported for this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PluginsAllowedForUrls
- GP name: Allow the Adobe Flash plug-in on specific sites (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\PluginsAllowedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\PluginsAllowedForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\PluginsAllowedForUrls\2 = "http://contoso.edu:8080"
```

Mac information and settings

- Preference Key Name: PluginsAllowedForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>http://contoso.edu:8080</string>
</array>
```

Back to top

PluginsBlockedForUrls

Block the Adobe Flash plug-in on specific sites (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 87.

Supported versions:

- On Windows and macOS since 77, until 87

Description

This policy doesn't work because Flash is no longer supported by Microsoft Edge.

Define a list of sites, based on URL patterns, that are blocked from running Adobe Flash.

If you don't configure this policy, the global default value from the DefaultPluginsSetting policy (if set) or the user's personal configuration is used for all sites.

For detailed information on valid url patterns, see https://go.microsoft.com/fwlink/?linkid=2095322. However, starting in M85, patterns with '*' and '[*.]' wildcards in the host are no longer supported for this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PluginsBlockedForUrls
- GP name: Block the Adobe Flash plug-in on specific sites (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\PluginsBlockedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\PluginsBlockedForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\PluginsBlockedForUrls\2 = "http://contoso.edu:8080"
```

Mac information and settings

- Preference Key Name: PluginsBlockedForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>http://contoso.edu:8080</string>
</array>
```

Back to top

PopupsAllowedForUrls

Allow pop-up windows on specific sites

Supported versions:

- On Windows and macOS since 77 or later

Description

Define a list of sites, based on URL patterns, that can open pop-up windows. * is not an accepted value for this policy.

If you don't configure this policy, the global default value from the DefaultPopupsSetting policy (if set) or the user's personal configuration is used for all sites.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PopupsAllowedForUrls
- GP name: Allow pop-up windows on specific sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\PopupsAllowedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\PopupsAllowedForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\PopupsAllowedForUrls\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: PopupsAllowedForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

PopupsBlockedForUrls

Block pop-up windows on specific sites

Supported versions:

- On Windows and macOS since 77 or later

Description

Define a list of sites, based on URL patterns, that are blocked from opening pop-up windows. * is not an accepted value for this policy.

If you don't configure this policy, the global default value from the DefaultPopupsSetting policy (if set) or the user's personal configuration is used for all sites.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PopupsBlockedForUrls
- GP name: Block pop-up windows on specific sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\PopupsBlockedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\PopupsBlockedForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\PopupsBlockedForUrls\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: PopupsBlockedForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

RegisteredProtocolHandlers

Register protocol handlers

Supported versions:

- On Windows and macOS since 77 or later

Description

Set this policy (recommended only) to register a list of protocol handlers. This list is merged with ones registered by the user and both are available to use.

To register a protocol handler:

- Set the protocol property to the scheme (for example, "mailto")
- Set the URL property to the URL property of the application that handlers the scheme specified in the "protocol" field. The pattern can include a "%s" placeholder, which the handled URL replaces.

Users can't remove a protocol handler registered by this policy. However, they can install a new default protocol handler to override the existing protocol handlers.

Supported features:

- Can be mandatory: No
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Dictionary

Windows information and settings

Group Policy (ADMX) info

- GP unique name: RegisteredProtocolHandlers
- GP name: Register protocol handlers
- GP path (Mandatory): N/A
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Content settings
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): N/A
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: RegisteredProtocolHandlers
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\RegisteredProtocolHandlers = [
  {
    "default": true,
    "protocol": "mailto",
    "url": "https://mail.contoso.com/mail/?extsrc=mailto&url=%s"
  }
]
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\RegisteredProtocolHandlers = [{"default": true, "protocol": "mailto",
"url": "https://mail.contoso.com/mail/?extsrc=mailto&url=%s"}]
```

Mac information and settings

- Preference Key Name: RegisteredProtocolHandlers
- Example value:

```
<key>RegisteredProtocolHandlers</key>
<array>
  <dict>
    <key>default</key>
    <true/>
    <key>protocol</key>
    <string>mailto</string>
    <key>url</key>
    <string>https://mail.contoso.com/mail/?extsrc=mailto&url=%s</string>
  </dict>
</array>
```

Back to top

SerialAllowAllPortsForUrls

Automatically grant sites permission to connect all serial ports

Supported versions:

- On Windows and macOS since 97 or later

Description

Setting the policy allows you to list sites which are automatically granted permission to access all available serial ports.

The URLs must be valid, or the policy is ignored. Only the origin (scheme, host, and port) of the URL is considered.

This policy overrides DefaultSerialGuardSetting, SerialAskForUrls, SerialBlockedForUrls and the user's preferences.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SerialAllowAllPortsForUrls
- GP name: Automatically grant sites permission to connect all serial ports
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\SerialAllowAllPortsForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\SerialAllowAllPortsForUrls\1 = "https://www.example.com"
```

Mac information and settings

- Preference Key Name: SerialAllowAllPortsForUrls
- Example value:

```
<array>
  <string>https://www.example.com</string>
</array>
```

Back to top

SerialAllowUsbDevicesForUrls

Automatically grant sites permission to connect to USB serial devices

Supported versions:

- On Windows and macOS since 97 or later

Description

Setting the policy lets you list sites that are automatically granted permission to access USB serial devices with vendor and product IDs that match the vendor_id and product_id fields.

Optionally you can omit the product_id field. This enables site access to all the vendor's devices. When you provide a product ID, then you give the site access to a specific device from the vendor but not all devices.

The URLs must be valid, or the policy is ignored. Only the origin (scheme, host, and port) of the URL is

considered.

This policy overrides DefaultSerialGuardSetting, SerialAskForUrls, SerialBlockedForUrls and the user's preferences.

This policy only affects access to USB devices through the Web Serial API. To grant access to USB devices through the WebUSB API see the WebUsbAllowDevicesForUrls policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Dictionary

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SerialAllowUsbDevicesForUrls
- GP name: Automatically grant sites permission to connect to USB serial devices
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: SerialAllowUsbDevicesForUrls
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\SerialAllowUsbDevicesForUrls = [
  {
    "devices": [
      {
        "product_id": 5678,
        "vendor_id": 1234
      }
    ],
    "urls": [
      "https://specific-device.example.com"
    ]
  },
  {
    "devices": [
      {
        "vendor_id": 1234
      }
    ],
    "urls": [
      "https://all-vendor-devices.example.com"
    ]
  }
]
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\SerialAllowUsbDevicesForUrls = [{"devices": [{"product_id": 5678,
"vendor_id": 1234}], "urls": ["https://specific-device.example.com"]}, {"devices": [{"vendor_id": 1234}],
"urls": ["https://all-vendor-devices.example.com"]}]
```

Mac information and settings

- Preference Key Name: SerialAllowUsbDevicesForUrls
- Example value:

```
<key>SerialAllowUsbDevicesForUrls</key>
<array>
  <dict>
    <key>devices</key>
    <array>
      <dict>
        <key>product_id</key>
        <integer>5678</integer>
        <key>vendor_id</key>
        <integer>1234</integer>
      </dict>
    </array>
    <key>urls</key>
    <array>
      <string>https://specific-device.example.com</string>
    </array>
  </dict>
  <dict>
    <key>devices</key>
    <array>
      <dict>
        <key>vendor_id</key>
        <integer>1234</integer>
      </dict>
    </array>
    <key>urls</key>
    <array>
      <string>https://all-vendor-devices.example.com</string>
    </array>
  </dict>
</array>
```

Back to top

ShowPDFDefaultRecommendationsEnabled

Allow notifications to set Microsoft Edge as default PDF reader

Supported versions:

- On Windows and macOS since 93 or later

Description

This policy setting lets you decide whether employees should receive recommendations to set Microsoft Edge as PDF handler.

If you enable or don't configure this setting, employees receive recommendations from Microsoft Edge to set itself as the default PDF handler.

If you disable this setting, employees will not receive any notifications from Microsoft Edge to set itself as the default PDF handler.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No

- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ShowPDFDefaultRecommendationsEnabled
- GP name: Allow notifications to set Microsoft Edge as default PDF reader
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ShowPDFDefaultRecommendationsEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ShowPDFDefaultRecommendationsEnabled
- Example value:

```
<true/>
```

Back to top

SpotlightExperiencesAndRecommendationsEnabled

Choose whether users can receive customized background images and text, suggestions, notifications, and tips for Microsoft services

Supported versions:

- On Windows since 86 or later

Description

Choose whether users can receive customized background images and text, suggestions, notifications, and tips for Microsoft services.

If you enable or don't configure this setting, spotlight experiences and recommendations are turned on.

If you disable this setting, spotlight experiences and recommendations are turned off.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SpotlightExperiencesAndRecommendationsEnabled
- GP name: Choose whether users can receive customized background images and text, suggestions,

notifications, and tips for Microsoft services

- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: SpotlightExperiencesAndRecommendationsEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

WebHidAskForUrls

Allow the WebHID API on these sites

Supported versions:

- On Windows and macOS since 100 or later

Description

Setting the policy lets you list the URL patterns that specify which sites can ask users to grant them access to a HID device.

Leaving the policy unset means DefaultWebHidGuardSetting applies for all sites, if it's set. If not, users' personal settings apply.

For URL patterns that don't match the policy, the following values are applied in order of precedence:

- WebHidBlockedForUrls (if there is a match),
- DefaultWebHidGuardSetting (if set), or
- Users' personal settings.

URL patterns must not conflict with WebHidBlockedForUrls. Neither policy takes precedence if a URL matches both patterns.

For detailed information about valid url patterns, see https://go.microsoft.com/fwlink/?linkid=2095322. * is not an accepted value for this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WebHidAskForUrls
- GP name: Allow the WebHID API on these sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\WebHidAskForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\WebHidAskForUrls\1 = "https://microsoft.com"
SOFTWARE\Policies\Microsoft\Edge\WebHidAskForUrls\2 = "https://chromium.org"
```

Mac information and settings

- Preference Key Name: WebHidAskForUrls
- Example value:

```
<array>
  <string>https://microsoft.com</string>
  <string>https://chromium.org</string>
</array>
```

Back to top

WebHidBlockedForUrls

Block the WebHID API on these sites

Supported versions:

- On Windows and macOS since 100 or later

Description

Setting the policy lets you list the URL patterns that specify which sites can't ask users to grant them access to a HID device.

Leaving the policy unset means DefaultWebHidGuardSetting applies for all sites, if it's set. If not, users' personal settings apply.

For URL patterns that don't match the policy, the following values are applied in order of precedence:

- WebHidAskForUrls (if there is a match),
- DefaultWebHidGuardSetting (if set), or
- Users' personal settings.

URL patterns can't conflict with WebHidAskForUrls. Neither policy takes precedence if a URL matches both patterns.

For detailed information about valid url patterns, see https://go.microsoft.com/fwlink/?linkid=2095322. * is not an accepted value for this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WebHidBlockedForUrls
- GP name: Block the WebHID API on these sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\WebHidBlockedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\WebHidBlockedForUrls\1 = "https://microsoft.com"
SOFTWARE\Policies\Microsoft\Edge\WebHidBlockedForUrls\2 = "https://chromium.org"
```

Mac information and settings

- Preference Key Name: WebHidBlockedForUrls
- Example value:

```
<array>
  <string>https://microsoft.com</string>
  <string>https://chromium.org</string>
</array>
```

Back to top

WebUsbAllowDevicesForUrls

Grant access to specific sites to connect to specific USB devices

Supported versions:

- On Windows and macOS since 77 or later

Description

Allows you to set a list of urls that specify which sites will automatically be granted permission to access a USB device with the given vendor and product IDs. Each item in the list must contain both devices and urls in order for the policy to be valid. Each item in devices can contain a vendor ID and product ID field. Any ID that is omitted is treated as a wildcard with one exception, and that exception is that a product ID cannot be specified without a vendor ID also being specified. Otherwise, the policy will not be valid and will be ignored.

The USB permission model uses the URL of the requesting site ("requesting URL") and the URL of the top-level frame site ("embedding URL") to grant permission to the requesting URL to access the USB device. The requesting URL may be different than the embedding URL when the requesting site is loaded in an iframe. Therefore, the "urls" field can contain up to two URL strings delimited by a comma to specify the requesting and embedding URL respectively. If only one URL is specified, then access to the corresponding USB devices will be granted when the requesting site's URL matches this URL regardless of embedding status. The URLs in "urls" must be valid URLs, otherwise the policy will be ignored.

If this policy is left not set, the global default value will be used for all sites either from the DefaultWebUsbGuardSetting policy if it is set, or the user's personal configuration otherwise.

URL patterns in this policy should not clash with the ones configured via WebUsbBlockedForUrls. If there is a clash, this policy will take precedence over WebUsbBlockedForUrls and WebUsbAskForUrls.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Dictionary

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WebUsbAllowDevicesForUrls
- GP name: Grant access to specific sites to connect to specific USB devices
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: WebUsbAllowDevicesForUrls
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\WebUsbAllowDevicesForUrls = [
  {
    "devices": [
      {
        "product_id": 5678,
        "vendor_id": 1234
      }
    ],
    "urls": [
      "https://contoso.com",
      "https://fabrikam.com"
    ]
  }
]
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\WebUsbAllowDevicesForUrls = [{"devices": [{"product_id": 5678, "vendor_id":
1234}], "urls": ["https://contoso.com", "https://fabrikam.com"]}]
```

Mac information and settings

- Preference Key Name: WebUsbAllowDevicesForUrls
- Example value:

```
<key>WebUsbAllowDevicesForUrls</key>
<array>
  <dict>
    <key>devices</key>
    <array>
      <dict>
        <key>product_id</key>
        <integer>5678</integer>
        <key>vendor_id</key>
        <integer>1234</integer>
      </dict>
    </array>
    <key>urls</key>
    <array>
      <string>https://contoso.com</string>
      <string>https://fabrikam.com</string>
    </array>
  </dict>
</array>
```

Back to top

WebUsbAskForUrls

Allow WebUSB on specific sites

Supported versions:

- On Windows and macOS since 77 or later

Description

Define a list of sites, based on URL patterns, that can ask the user for access to a USB device.

If you don't configure this policy, the global default value from the DefaultWebUsbGuardSetting policy (if set) or the user's personal configuration is used for all sites.

The URL patterns defined in this policy can't conflict with those configured in the WebUsbBlockedForUrls policy - you can't both allow and block a URL. For detailed information on valid url patterns, please see https://go.microsoft.com/fwlink/?linkid=2095322

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WebUsbAskForUrls
- GP name: Allow WebUSB on specific sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\WebUsbAskForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\WebUsbAskForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\WebUsbAskForUrls\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: WebUsbAskForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

WebUsbBlockedForUrls

Block WebUSB on specific sites

Supported versions:

- On Windows and macOS since 77 or later

Description

Define a list of sites, based on URL patterns, that can't ask the user to grant them access to a USB device.

If you don't configure this policy, the global default value from the DefaultWebUsbGuardSetting policy (if set) or the user's personal configuration is used for all sites.

URL patterns in this policy can't conflict with those configured in the WebUsbAskForUrls policy. You can't both allow and block a URL. For detailed information on valid url patterns, see https://go.microsoft.com/fwlink/?linkid=2095322.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WebUsbBlockedForUrls
- GP name: Block WebUSB on specific sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Content settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\WebUsbBlockedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\WebUsbBlockedForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\WebUsbBlockedForUrls\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: WebUsbBlockedForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

Default search provider policies

Back to top

DefaultSearchProviderEnabled

Enable the default search provider

Supported versions:

- On Windows and macOS since 77 or later

Description

Enables the ability to use a default search provider.

If you enable this policy, a user can search for a term by typing in the address bar (as long as what they type isn't a URL).

You can specify the default search provider to use by enabling the rest of the default search policies. If these are left empty (not configured) or configured incorrectly, the user can choose the default provider.

If you disable this policy, the user can't search from the address bar.

If you enable or disable this policy, users can't change or override it.

If you don't configure this policy, the default search provider is enabled, and the user can choose the default search provider and set the search provider list.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management, or macOS instances that are that are managed via MDM or joined to a domain via MCX..

Starting in Microsoft Edge 84, you can set this policy as a recommended policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultSearchProviderEnabled
- GP name: Enable the default search provider

- GP path (Mandatory): Administrative Templates/Microsoft Edge/Default search provider
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Default search provider
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: DefaultSearchProviderEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: DefaultSearchProviderEnabled
- Example value:

```
<true/>
```

Back to top

DefaultSearchProviderEncodings

Default search provider encodings

Supported versions:

- On Windows and macOS since 77 or later

Description

Specify the character encodings supported by the search provider. Encodings are code page names like UTF-8, GB2312, and ISO-8859-1. They are tried in the order provided.

This policy is optional. If not configured, the default, UTF-8, is used.

This policy is applied only if you enable the DefaultSearchProviderEnabled and DefaultSearchProviderSearchURL policies.

Starting in Microsoft Edge 84, you can set this policy as a recommended policy. If the user has already set a default search provider, the default search provider configured by this recommended policy will not be added to the list of search providers the user can choose from. If this is the desired behavior, use the ManagedSearchEngines policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultSearchProviderEncodings
- GP name: Default search provider encodings
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Default search provider

- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Default search provider
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\DefaultSearchProviderEncodings
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended\DefaultSearchProviderEncodings
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\DefaultSearchProviderEncodings\1 = "UTF-8"
SOFTWARE\Policies\Microsoft\Edge\DefaultSearchProviderEncodings\2 = "UTF-16"
SOFTWARE\Policies\Microsoft\Edge\DefaultSearchProviderEncodings\3 = "GB2312"
SOFTWARE\Policies\Microsoft\Edge\DefaultSearchProviderEncodings\4 = "ISO-8859-1"
```

Mac information and settings

- Preference Key Name: DefaultSearchProviderEncodings
- Example value:

```
<array>
  <string>UTF-8</string>
  <string>UTF-16</string>
  <string>GB2312</string>
  <string>ISO-8859-1</string>
</array>
```

Back to top

DefaultSearchProviderImageURL

Specifies the search-by-image feature for the default search provider

Supported versions:

- On Windows and macOS since 77 or later

Description

Specifies the URL to the search engine used for image search. Search requests are sent using the GET method.

This policy is optional. If you don't configure it, image search isn't available.

Specify Bing's Image Search URL as: '{bing:baseURL}images/detail/search?iss=sbiupload&FORM=ANCMS1#enterInsights'.

Specify Google's Image Search URL as: '{google:baseURL}searchbyimage/upload'.

See DefaultSearchProviderImageURLPostParams policy to finish configuring image search.

This policy is applied only if you enable the DefaultSearchProviderEnabled and DefaultSearchProviderSearchURL policies.

Starting in Microsoft Edge 84, you can set this policy as a recommended policy. If the user has already set a default search provider, the default search provider configured by this recommended policy will not be added to the list of search providers the user can choose from. If this is the desired behavior, use the ManagedSearchEngines policy.

Supported features:

- Can be mandatory: Yes

- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultSearchProviderImageURL
- GP name: Specifies the search-by-image feature for the default search provider
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Default search provider
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Default search provider
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: DefaultSearchProviderImageURL
- Value Type: REG_SZ

Example value:

```
"https://search.contoso.com/searchbyimage/upload"
```

Mac information and settings

- Preference Key Name: DefaultSearchProviderImageURL
- Example value:

```
<string>https://search.contoso.com/searchbyimage/upload</string>
```

Back to top

DefaultSearchProviderImageURLPostParams

Parameters for an image URL that uses POST

Supported versions:

- On Windows and macOS since 77 or later

Description

If you enable this policy, it specifies the parameters used when an image search that uses POST is performed. The policy consists of comma-separated name/value pairs. If a value is a template parameter, like {imageThumbnail} in the preceding example, it's replaced with real image thumbnail data. This policy is applied only if you enable the DefaultSearchProviderEnabled and DefaultSearchProviderSearchURL policies.

Specify Bing's Image Search URL Post Params as: 'imageBin={google:imageThumbnailBase64}'.

Specify Google's Image Search URL Post Params as: 'encoded_image={google:imageThumbnail},image_url={google:imageURL},sbisrc={google:imageSearchSource},original_width={google:imageOriginalWidth},original_height={google:imageOriginalHeight}'.

If you don't set this policy, image search requests are sent using the GET method.

Starting in Microsoft Edge 84, you can set this policy as a recommended policy. If the user has already set a default search provider, the default search provider configured by this recommended policy will not be added to the list of search providers the user can choose from. If this is the desired behavior, use the ManagedSearchEngines policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultSearchProviderImageURLPostParams
- GP name: Parameters for an image URL that uses POST
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Default search provider
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Default search provider
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: DefaultSearchProviderImageURLPostParams
- Value Type: REG_SZ

Example value:

```
"content={imageThumbnail},url={imageURL},sbisrc={SearchSource}"
```

Mac information and settings

- Preference Key Name: DefaultSearchProviderImageURLPostParams
- Example value:

```
<string>content={imageThumbnail},url={imageURL},sbisrc={SearchSource}</string>
```

Back to top

DefaultSearchProviderKeyword

Default search provider keyword

Supported versions:

- On Windows and macOS since 77 or later

Description

Specifies the keyword, which is the shortcut used in the Address Bar to trigger the search for this provider.

This policy is optional. If you don't configure it, no keyword activates the search provider.

This policy is applied only if you enable the DefaultSearchProviderEnabled and DefaultSearchProviderSearchURL policies.

Starting in Microsoft Edge 84, you can set this policy as a recommended policy. If the user has already set a default search provider, the default search provider configured by this recommended policy will not be added to the list of search providers the user can choose from. If this is the desired behavior, use the ManagedSearchEngines policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes

- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultSearchProviderKeyword
- GP name: Default search provider keyword
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Default search provider
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Default search provider
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: DefaultSearchProviderKeyword
- Value Type: REG_SZ

Example value:

```
"mis"
```

Mac information and settings

- Preference Key Name: DefaultSearchProviderKeyword
- Example value:

```
<string>mis</string>
```

Back to top

DefaultSearchProviderName

Default search provider name

Supported versions:

- On Windows and macOS since 77 or later

Description

Specifies the name of the default search provider.

If you enable this policy, you set the name of the default search provider.

If you don't enable this policy or if you leave it empty, the host name specified by the search URL is used.

'DefaultSearchProviderName' should be set to an organization-approved encrypted search provider that corresponds to the encrypted search provider set in DTBC-0008. This policy is applied only if you enable the DefaultSearchProviderEnabled and DefaultSearchProviderSearchURL policies.

Starting in Microsoft Edge 84, you can set this policy as a recommended policy. If the user has already set a default search provider, the default search provider configured by this recommended policy will not be added to the list of search providers the user can choose from. If this is the desired behavior, use the ManagedSearchEngines policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes

- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultSearchProviderName
- GP name: Default search provider name
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Default search provider
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Default search provider
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: DefaultSearchProviderName
- Value Type: REG_SZ

Example value:

```
"My Intranet Search"
```

Mac information and settings

- Preference Key Name: DefaultSearchProviderName
- Example value:

```
<string>My Intranet Search</string>
```

Back to top

DefaultSearchProviderSearchURL

Default search provider search URL

Supported versions:

- On Windows and macOS since 77 or later

Description

Specifies the URL of the search engine used for a default search. The URL contains the string '{searchTerms}', which is replaced at query time by the terms the user is searching for.

Specify Bing's search URL as:

'{bing:baseURL}search?q={searchTerms}'.

Specify Google's search URL as: '{google:baseURL}search?q={searchTerms}&{google:RLZ}{google:originalQueryForSuggestion}{google:assistedQueryStats}{google:searchFieldtrialParameter}{google:searchClient}{google:sourceId}ie={inputEncoding}'.

This policy is required when you enable the DefaultSearchProviderEnabled policy; if you don't enable the latter policy, this policy is ignored.

Starting in Microsoft Edge 84, you can set this policy as a recommended policy. If the user has already set a default search provider, the default search provider configured by this recommended policy will not be added to the list of search providers the user can choose from. If this is the desired behavior, use the ManagedSearchEngines policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultSearchProviderSearchURL
- GP name: Default search provider search URL
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Default search provider
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Default search provider
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: DefaultSearchProviderSearchURL
- Value Type: REG_SZ

Example value:

```
"https://search.contoso.com/search?q={searchTerms}"
```

Mac information and settings

- Preference Key Name: DefaultSearchProviderSearchURL
- Example value:

```
<string>https://search.contoso.com/search?q={searchTerms}</string>
```

Back to top

DefaultSearchProviderSuggestURL

Default search provider URL for suggestions

Supported versions:

- On Windows and macOS since 77 or later

Description

Specifies the URL for the search engine used to provide search suggestions. The URL contains the string '{searchTerms}', which is replaced at query time by the text the user has entered so far.

This policy is optional. If you don't configure it, users won't see search suggestions; they will see suggestions from their browsing history and favorites.

Bing's suggest URL can be specified as:

'{bing:baseURL}qbox?query={searchTerms}'.

Google's suggest URL can be specified as: '{google:baseURL}complete/search?output=chrome&q={searchTerms}'.

This policy is applied only if you enable the DefaultSearchProviderEnabled and DefaultSearchProviderSearchURL policies.

Starting in Microsoft Edge 84, you can set this policy as a recommended policy. If the user has already set a default search provider, the default search provider configured by this recommended policy will not be added to the list of search providers the user can choose from. If this is the desired behavior, use the ManagedSearchEngines policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultSearchProviderSuggestURL
- GP name: Default search provider URL for suggestions
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Default search provider
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Default search provider
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: DefaultSearchProviderSuggestURL
- Value Type: REG_SZ

Example value:

```
"https://search.contoso.com/suggest?q={searchTerms}"
```

Mac information and settings

- Preference Key Name: DefaultSearchProviderSuggestURL
- Example value:

```
<string>https://search.contoso.com/suggest?q={searchTerms}</string>
```

Back to top

NewTabPageSearchBox

Configure the new tab page search box experience

Supported versions:

- On Windows and macOS since 85 or later

Description

You can configure the new tab page search box to use "Search box (Recommended)" or "Address bar" to search on new tabs. This policy only works if you set the search engine to a value other than Bing by setting the following two policies: DefaultSearchProviderEnabled and DefaultSearchProviderSearchURL.

If you disable or don't configure this policy and:

- If the address bar default search engine is Bing, the new tab page uses the search box to search on new tabs.
- If the address bar default search engine is not Bing, users are offered an additional choice (use "Address bar") when searching on new tabs.

If you enable this policy and set it to:

- "Search box (Recommended)" ('bing'), the new tab page uses the search box to search on new tabs.
- "Address bar" ('redirect'), the new tab page search box uses the address bar to search on new tabs.

Policy options mapping:

- bing (bing) = Search box (Recommended)
- redirect (redirect) = Address bar

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NewTabPageSearchBox
- GP name: Configure the new tab page search box experience
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Default search provider
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Default search provider
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: NewTabPageSearchBox
- Value Type: REG_SZ

Example value:

```
"bing"
```

Mac information and settings

- Preference Key Name: NewTabPageSearchBox
- Example value:

```
<string>bing</string>
```

Back to top

Edge Workspaces settings policies

Back to top

EdgeWorkspacesEnabled

Enable Workspaces

Supported versions:

- On Windows and macOS since 106 or later

Description

Microsoft Edge Workspaces helps improve productivity for users in your organization.

If you enable this policy, users will be able to access the Microsoft Edge Workspaces feature. If you disable or don't configure this policy, users will not be able to access the Microsoft Edge Workspaces feature.

To learn more about the feature, see https://go.microsoft.com/fwlink/?linkid=2209950

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EdgeWorkspacesEnabled
- GP name: Enable Workspaces
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Edge Workspaces settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: EdgeWorkspacesEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: EdgeWorkspacesEnabled
- Example value:

```
<true/>
```

Back to top

Experimentation policies

Back to top

FeatureFlagOverridesControl

Configure users ability to override feature flags

Supported versions:

- On Windows and macOS since 93 or later

Description

Configures users ability to override state of feature flags. If you set this policy to 'CommandLineOverridesEnabled', users can override state of feature flags using command line arguments but not edge://flags page.

If you set this policy to 'OverridesEnabled', users can override state of feature flags using command line arguments or edge://flags page.

If you set this policy to 'OverridesDisabled', users can't override state of feature flags using command line arguments or edge://flags page.

If you don't configure this policy, the behavior is the same as the 'OverridesEnabled'.

Policy options mapping:

- CommandLineOverridesEnabled (2) = Allow users to override feature flags using command line arguments only
- OverridesEnabled (1) = Allow users to override feature flags
- OverridesDisabled (0) = Prevent users from overriding feature flags

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: FeatureFlagOverridesControl
- GP name: Configure users ability to override feature flags
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Experimentation
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: FeatureFlagOverridesControl
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: FeatureFlagOverridesControl
- Example value:

```
<integer>1</integer>
```

Back to top

Extensions policies

Back to top

BlockExternalExtensions

Blocks external extensions from being installed

Supported versions:

- On Windows and macOS since 88 or later

Description

Control the installation of external extensions.

If you enable this setting, external extensions are blocked from being installed.

If you disable this setting or leave it unset, external extensions are allowed to be installed.

External extensions and their installation are documented at Alternate extension distribution methods.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: BlockExternalExtensions
- GP name: Blocks external extensions from being installed
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Extensions
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: BlockExternalExtensions
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: BlockExternalExtensions
- Example value:

```
<true/>
```

Back to top

ControlDefaultStateOfAllowExtensionFromOtherStoresSettingEnabled

Configure default state of Allow extensions from other stores setting

Supported versions:

- On Windows and macOS since 101 or later

Description

This policy allows you to control the default state of the Allow extensions from other stores setting. This policy can't be used to stop installation of extensions from other stores such as Chrome Web Store. To stop installation

of extensions from other stores, use the Extension Settings policy: https://go.microsoft.com/fwlink/?linkid=2187098.

When enabled, Allow extensions from other stores will be turned on. So, users won't have to turn on the flag manually while installing extensions from other supported stores such as Chrome Web Store. However a user can override this setting. If the user has already turned on the setting and then turned it off, this setting may not work. If the Admin first sets the policy as Enabled, but then changes it to not configured or disabled, it will have no impact on user settings and the setting will remain as it is.

When disabled or not configured, the user can manage the Allow extensions from other store setting.

Supported features:

- Can be mandatory: No
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ControlDefaultStateOfAllowExtensionFromOtherStoresSettingEnabled
- GP name: Configure default state of Allow extensions from other stores setting
- GP path (Mandatory): N/A
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Extensions
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): N/A
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ControlDefaultStateOfAllowExtensionFromOtherStoresSettingEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ControlDefaultStateOfAllowExtensionFromOtherStoresSettingEnabled
- Example value:

```
<true/>
```

Back to top

ExtensionAllowedTypes

Configure allowed extension types

Supported versions:

- On Windows and macOS since 77 or later

Description

Setting the policy controls which apps and extensions may be installed in Microsoft Edge, which hosts they can interact with, and limits runtime access.

If you don't set this policy, there aren't any restrictions on acceptable extension and app types.

Extensions and apps which have a type that's not on the list won't be installed. Each value should be one of these strings:

- "extension"
- "theme"
- "user_script"
- "hosted_app"

See the Microsoft Edge extensions documentation for more information about these types.

Note: This policy also affects extensions and apps to be force-installed using ExtensionInstallForcelist.

Policy options mapping:

- extension (extension) = Extension
- theme (theme) = Theme
- user_script (user_script) = User script
- hosted_app (hosted_app) = Hosted app
- legacy_packaged_app (legacy_packaged_app) = Legacy packaged app
- platform_app (platform_app) = Platform app

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ExtensionAllowedTypes
- GP name: Configure allowed extension types
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Extensions
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\ExtensionAllowedTypes
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ExtensionAllowedTypes\1 = "hosted_app"
```

Mac information and settings

- Preference Key Name: ExtensionAllowedTypes

- Example value:

```
<array>
  <string>hosted_app</string>
</array>
```

Back to top

ExtensionInstallAllowlist

Allow specific extensions to be installed

Supported versions:

- On Windows and macOS since 77 or later

Description

Setting this policy specifies which extensions are not subject to the blocklist.

A blocklist value of * means all extensions are blocked and users can only install extensions listed in the allow list.

By default, all extensions are allowed. However, if you prohibited extensions by policy, you can use the list of allowed extensions to change that policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ExtensionInstallAllowlist
- GP name: Allow specific extensions to be installed
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Extensions
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\ExtensionInstallAllowlist
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ExtensionInstallAllowlist\1 = "extension_id1"
SOFTWARE\Policies\Microsoft\Edge\ExtensionInstallAllowlist\2 = "extension_id2"
```

Mac information and settings

- Preference Key Name: ExtensionInstallAllowlist
- Example value:

```
<array>
  <string>extension_id1</string>
  <string>extension_id2</string>
</array>
```

Back to top

ExtensionInstallBlocklist

Control which extensions cannot be installed

Supported versions:

- On Windows and macOS since 77 or later

Description

Lets you specify which extensions the users CANNOT install. Extensions already installed will be disabled if blocked, without a way for the user to enable them. After a disabled extension is removed from the blocklist it will automatically get re-enabled.

A blocklist value of '*' means all extensions are blocked unless they are explicitly listed in the allowlist.

If this policy isn't set, the user can install any extension in Microsoft Edge.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ExtensionInstallBlocklist
- GP name: Control which extensions cannot be installed
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Extensions
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\ExtensionInstallBlocklist
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ExtensionInstallBlocklist\1 = "extension_id1"
SOFTWARE\Policies\Microsoft\Edge\ExtensionInstallBlocklist\2 = "extension_id2"
```

Mac information and settings

- Preference Key Name: ExtensionInstallBlocklist
- Example value:

```
<array>
  <string>extension_id1</string>
  <string>extension_id2</string>
</array>
```

Back to top

ExtensionInstallForcelist

Control which extensions are installed silently

Supported versions:

- On Windows and macOS since 77 or later

Description

Set this policy to specify a list of apps and extensions that install silently, without user interaction. Users can't uninstall or turn off this setting. Permissions are granted implicitly, including the enterprise.deviceAttributes and enterprise.platformKeys extension APIs. Note: These 2 APIs aren't available to apps and extensions that aren't force-installed.

If you don't set this policy, no apps or extensions are autoinstalled and users can uninstall any app in Microsoft Edge.

This policy supercedes ExtensionInstallBlocklist policy. If a previously force-installed app or extension is removed from this list, Microsoft Edge automatically uninstalls it.

For Windows instances not joined to a Microsoft Active Directory domain, forced installation is limited to apps and extensions listed in the Microsoft Edge Add-ons website.

On macOS instances, apps and extensions from outside the Microsoft Edge Add-ons website can only be force installed if the instance is managed via MDM, or joined to a domain via MCX.

The source code of any extension can be altered by users with developer tools, potentially rendering the extension unfunctional. If this is a concern, configure the DeveloperToolsAvailability policy.

Each list item of the policy is a string that contains an extension ID and, optionally, an "update" URL separated by a semicolon (;). The extension ID is the 32-letter string found, for example, on edge://extensions when in Developer mode. If specified, the "update" URL should point to an Update Manifest XML document (https://go.microsoft.com/fwlink/?linkid=2095043). By default, the Microsoft Edge Add-ons website's update URL is used. The "update" URL set in this policy is only used for the initial installation; subsequent updates of the extension use the update URL in the extension's manifest.

Note: This policy doesn't apply to InPrivate mode. Read about hosting extensions at Publish and update extensions in the Microsoft Edge Add-ons website.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ExtensionInstallForcelist
- GP name: Control which extensions are installed silently
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Extensions
- GP path (Recommended): N/A

- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\ExtensionInstallForcelist
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ExtensionInstallForcelist\1 =
"gbchcmhmhahfdphkhkmpfmihenigjmpp;https://edge.microsoft.com/extensionwebstorebase/v1/crx"
SOFTWARE\Policies\Microsoft\Edge\ExtensionInstallForcelist\2 = "abcdefghijklmnopabcdefghijklmnop"
```

Mac information and settings

- Preference Key Name: ExtensionInstallForcelist
- Example value:

```
<array>
  <string>gbchcmhmhahfdphkhkmpfmihenigjmpp;https://edge.microsoft.com/extensionwebstorebase/v1/crx</string>
  <string>abcdefghijklmnopabcdefghijklmnop</string>
</array>
```

Back to top

ExtensionInstallSources

Configure extension and user script install sources

Supported versions:

- On Windows and macOS since 77 or later

Description

Define URLs that can install extensions and themes.

Define URLs that can install extensions and themes directly without having to drag and drop the packages to the edge://extensions page.

Each item in this list is an extension-style match pattern (see https://go.microsoft.com/fwlink/?linkid=2095039). Users can easily install items from any URL that matches an item in this list. Both the location of the *.crx file and the page where the download is started from (in other words, the referrer) must be allowed by these patterns. Do not host the files at a location that requires authentication.

The ExtensionInstallBlocklist policy takes precedence over this policy. Any extensions that's on the block list won't be installed, even if it comes from a site on this list.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ExtensionInstallSources
- GP name: Configure extension and user script install sources

- GP path (Mandatory): Administrative Templates/Microsoft Edge/Extensions
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\ExtensionInstallSources
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ExtensionInstallSources\1 = "https://corp.contoso.com/*"
```

Mac information and settings

- Preference Key Name: ExtensionInstallSources
- Example value:

```
<array>
  <string>https://corp.contoso.com/*</string>
</array>
```

Back to top

ExtensionSettings

Configure extension management settings

Supported versions:

- On Windows and macOS since 77 or later

Description

Setting this policy controls extension management settings for Microsoft Edge, including any controlled by existing extension-related policies. This policy supersedes any legacy policies that might be set.

This policy maps an extension ID or an update URL to its specific setting only. A default configuration can be set for the special ID "*", which applies to all extensions without a custom configuration in this policy. With an update URL, configuration applies to extensions with the exact update URL stated in the extension manifest. If the 'override_update_url' flag is set to true, the extension is installed and updated using the update URL specified in the ExtensionInstallForcelist policy or in 'update_url' field in this policy. The flag 'override_update_url' is ignored if the 'update_url' is the Edge Add-ons website update URL. For more details, check out the detailed guide to ExtensionSettings policy available at https://go.microsoft.com/fwlink/?linkid=2161555.

To block extensions from a particular third party store, you only need to block the update_url for that store. For example, if you want to block extensions from Chrome Web Store, you can use the following JSON.

{"update_url:https://clients2.google.com/service/update2/crx":{"installation_mode":"blocked"}}

Note that you can still use ExtensionInstallForcelist and ExtensionInstallAllowlist to allow / force install specific extensions even if the store is blocked using the JSON in the previous example.

Note: For Windows instances not joined to a Microsoft Active Directory domain and macOS instances not managed via MDM or joined to a domain via MCX, forced installation is limited to apps and extensions listed in the Microsoft Edge Add-ons website.

Supported features:

- Can be mandatory: Yes

- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Dictionary

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ExtensionSettings
- GP name: Configure extension management settings
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Extensions
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ExtensionSettings
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ExtensionSettings = {
  "*": {
    "allowed_types": [
      "hosted_app"
    ],
    "blocked_install_message": "Custom error message.",
    "blocked_permissions": [
      "downloads",
      "bookmarks"
    ],
    "install_sources": [
      "https://company-intranet/apps"
    ],
    "installation_mode": "blocked",
    "runtime_allowed_hosts": [
      "*://good.contoso.com"
    ],
    "runtime_blocked_hosts": [
      "*://*.contoso.com"
    ]
  },
  "abcdefghijklmnopabcdefghijklmnop": {
    "blocked_permissions": [
      "history"
    ],
    "installation_mode": "allowed",
    "minimum_version_required": "1.0.1"
  },
  "bcdefghijklmnopabcdefghijklmnopa": {
    "allowed_permissions": [
      "downloads"
    ],
    "installation_mode": "force_installed",
    "override_update_url": true,
    "runtime_allowed_hosts": [
      "*://good.contoso.com"
    ],
    "runtime_blocked_hosts": [
      "*://*.contoso.com"
    ],
    "toolbar_state": "force_shown",
    "update_url": "https://contoso.com/update_url"
  },
  "cdefghijklmnopabcdefghijklmnopab": {
    "blocked_install_message": "Custom error message.",
    "installation_mode": "blocked"
  },
  "defghijklmnopabcdefghijklmnopabc,efghijklmnopabcdefghijklmnopabcd": {
    "blocked_install_message": "Custom error message.",
    "installation_mode": "blocked"
  },
  "fghijklmnopabcdefghijklmnopabcde": {
    "blocked_install_message": "Custom removal message.",
    "installation_mode": "removed"
  },
  "update_url:https://www.contoso.com/update.xml": {
    "allowed_permissions": [
      "downloads"
    ],
    "blocked_permissions": [
      "wallpaper"
    ],
    "installation_mode": "allowed"
  }
}
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\ExtensionSettings = {"*": {"allowed_types": ["hosted_app"],
"blocked_install_message": "Custom error message.", "blocked_permissions": ["downloads", "bookmarks"],
"install_sources": ["https://company-intranet/apps"], "installation_mode": "blocked",
"runtime_allowed_hosts": ["*://good.contoso.com"], "runtime_blocked_hosts": ["*://*.contoso.com"]},
"abcdefghijklmnopabcdefghijklmnop": {"blocked_permissions": ["history"], "installation_mode": "allowed",
"minimum_version_required": "1.0.1"}, "bcdefghijklmnopabcdefghijklmnopa": {"allowed_permissions":
["downloads"], "installation_mode": "force_installed", "override_update_url": true, "runtime_allowed_hosts":
["*://good.contoso.com"], "runtime_blocked_hosts": ["*://*.contoso.com"], "toolbar_state": "force_shown",
"update_url": "https://contoso.com/update_url"}, "cdefghijklmnopabcdefghijklmnopab":
{"blocked_install_message": "Custom error message.", "installation_mode": "blocked"},
"defghijklmnopabcdefghijklmnopabc,efghijklmnopabcdefghijklmnopabcd": {"blocked_install_message": "Custom
error message.", "installation_mode": "blocked"}, "fghijklmnopabcdefghijklmnopabcde":
{"blocked_install_message": "Custom removal message.", "installation_mode": "removed"},
"update_url:https://www.contoso.com/update.xml": {"allowed_permissions": ["downloads"],
"blocked_permissions": ["wallpaper"], "installation_mode": "allowed"}}
```

Mac information and settings

- Preference Key Name: ExtensionSettings
- Example value:

```
<key>ExtensionSettings</key>
<dict>
  <key>*</key>
  <dict>
    <key>allowed_types</key>
    <array>
      <string>hosted_app</string>
    </array>
    <key>blocked_install_message</key>
    <string>Custom error message.</string>
    <key>blocked_permissions</key>
    <array>
      <string>downloads</string>
      <string>bookmarks</string>
    </array>
    <key>install_sources</key>
    <array>
      <string>https://company-intranet/apps</string>
    </array>
    <key>installation_mode</key>
    <string>blocked</string>
    <key>runtime_allowed_hosts</key>
    <array>
      <string>*://good.contoso.com</string>
    </array>
    <key>runtime_blocked_hosts</key>
    <array>
      <string>*://*.contoso.com</string>
    </array>
  </dict>
  <key>abcdefghijklmnopabcdefghijklmnop</key>
  <dict>
    <key>blocked_permissions</key>
    <array>
      <string>history</string>
    </array>
    <key>installation_mode</key>
    <string>allowed</string>
    <key>minimum_version_required</key>
    <string>1.0.1</string>
  </dict>
  <key>bcdefghijklmnopabcdefghijklmnopa</key>
  <dict>
    <key>allowed_permissions</key>
    <array>
```

```
      <string>downloads</string>
    </array>
    <key>installation_mode</key>
    <string>force_installed</string>
    <key>override_update_url</key>
    <true/>
    <key>runtime_allowed_hosts</key>
    <array>
      <string>*://good.contoso.com</string>
    </array>
    <key>runtime_blocked_hosts</key>
    <array>
      <string>*://*.contoso.com</string>
    </array>
    <key>toolbar_state</key>
    <string>force_shown</string>
    <key>update_url</key>
    <string>https://contoso.com/update_url</string>
  </dict>
  <key>cdefghijklmnopabcdefghijklmnopab</key>
  <dict>
    <key>blocked_install_message</key>
    <string>Custom error message.</string>
    <key>installation_mode</key>
    <string>blocked</string>
  </dict>
  <key>defghijklmnopabcdefghijklmnopabc,efghijklmnopabcdefghijklmnopabcd</key>
  <dict>
    <key>blocked_install_message</key>
    <string>Custom error message.</string>
    <key>installation_mode</key>
    <string>blocked</string>
  </dict>
  <key>fghijklmnopabcdefghijklmnopabcde</key>
  <dict>
    <key>blocked_install_message</key>
    <string>Custom removal message.</string>
    <key>installation_mode</key>
    <string>removed</string>
  </dict>
  <key>update_url:https://www.contoso.com/update.xml</key>
  <dict>
    <key>allowed_permissions</key>
    <array>
      <string>downloads</string>
    </array>
    <key>blocked_permissions</key>
    <array>
      <string>wallpaper</string>
    </array>
    <key>installation_mode</key>
    <string>allowed</string>
  </dict>
</dict>
```

Back to top

HTTP authentication policies

Back to top

AllHttpAuthSchemesAllowedForOrigins

List of origins that allow all HTTP authentication

Supported versions:

- On Windows and macOS since 102 or later

Description

Set this policy to specify which origins allow all the HTTP authentication schemes Microsoft Edge supports regardless of the AuthSchemes policy.

Format the origin pattern according to this format (https://www.chromium.org/administrators/url-blocklist-filter-format). Up to 1,000 exceptions can be defined in AllHttpAuthSchemesAllowedForOrigins. Wildcards are allowed for the whole origin or parts of the origin. Parts include the scheme, host, or port.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AllHttpAuthSchemesAllowedForOrigins
- GP name: List of origins that allow all HTTP authentication
- GP path (Mandatory): Administrative Templates/Microsoft Edge/HTTP authentication
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\AllHttpAuthSchemesAllowedForOrigins
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\AllHttpAuthSchemesAllowedForOrigins\1 = "*.example.com"
```

Mac information and settings

- Preference Key Name: AllHttpAuthSchemesAllowedForOrigins
- Example value:

```
<array>
  <string>*.example.com</string>
</array>
```

Back to top

AllowCrossOriginAuthPrompt

Allow cross-origin HTTP Authentication prompts

Supported versions:

- On Windows and macOS since 77 or later

Description

Controls whether third-party images on a page can show an authentication prompt.

Typically, this is disabled as a phishing defense. If you don't configure this policy, it's disabled and third-party images can't show an authentication prompt.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AllowCrossOriginAuthPrompt
- GP name: Allow cross-origin HTTP Authentication prompts
- GP path (Mandatory): Administrative Templates/Microsoft Edge/HTTP authentication
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AllowCrossOriginAuthPrompt
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: AllowCrossOriginAuthPrompt
- Example value:

```
<false/>
```

Back to top

AuthNegotiateDelegateAllowlist

Specifies a list of servers that Microsoft Edge can delegate user credentials to

Supported versions:

- On Windows and macOS since 77 or later

Description

Configure the list of servers that Microsoft Edge can delegate to.

Separate multiple server names with commas. Wildcards (*) are allowed.

If you don't configure this policy Microsoft Edge won't delegate user credentials even if a server is detected as Intranet.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AuthNegotiateDelegateAllowlist
- GP name: Specifies a list of servers that Microsoft Edge can delegate user credentials to
- GP path (Mandatory): Administrative Templates/Microsoft Edge/HTTP authentication
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AuthNegotiateDelegateAllowlist
- Value Type: REG_SZ

Example value:

```
"contoso.com"
```

Mac information and settings

- Preference Key Name: AuthNegotiateDelegateAllowlist
- Example value:

```
<string>contoso.com</string>
```

Back to top

AuthSchemes

Supported authentication schemes

Supported versions:

- On Windows and macOS since 77 or later

Description

Specifies which HTTP authentication schemes are supported.

You can configure the policy by using these values: 'basic', 'digest', 'ntlm', and 'negotiate'. Separate multiple values with commas.

Note: All values for this policy are case sensitive.

If you don't configure this policy, all four schemes are used.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AuthSchemes
- GP name: Supported authentication schemes
- GP path (Mandatory): Administrative Templates/Microsoft Edge/HTTP authentication
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AuthSchemes
- Value Type: REG_SZ

Example value:

```
"basic,digest,ntlm,negotiate"
```

Mac information and settings

- Preference Key Name: AuthSchemes
- Example value:

```
<string>basic,digest,ntlm,negotiate</string>
```

Back to top

AuthServerAllowlist

Configure list of allowed authentication servers

Supported versions:

- On Windows and macOS since 77 or later

Description

Specifies which servers to enable for integrated authentication. Integrated authentication is only enabled when Microsoft Edge receives an authentication challenge from a proxy or from a server in this list.

Separate multiple server names with commas. Wildcards (*) are allowed.

If you don't configure this policy, Microsoft Edge tries to detect if a server is on the intranet - only then will it respond to IWA requests. If the server is on the internet, IWA requests from it are ignored by Microsoft Edge.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AuthServerAllowlist
- GP name: Configure list of allowed authentication servers
- GP path (Mandatory): Administrative Templates/Microsoft Edge/HTTP authentication
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AuthServerAllowlist
- Value Type: REG_SZ

Example value:

```
"*contoso.com,contoso.com"
```

Mac information and settings

- Preference Key Name: AuthServerAllowlist
- Example value:

```
<string>*contoso.com,contoso.com</string>
```

Back to top

BasicAuthOverHttpEnabled

Allow Basic authentication for HTTP

Supported versions:

- On Windows and macOS since 88 or later

Description

If you enable this policy or leave it unset, Basic authentication challenges received over non-secure HTTP will be allowed.

If you disable this policy, non-secure HTTP requests from the Basic authentication scheme are blocked, and only secure HTTPS is allowed.

This policy setting is ignored (and Basic is always forbidden) if the AuthSchemes policy is set and does not include Basic.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: BasicAuthOverHttpEnabled
- GP name: Allow Basic authentication for HTTP
- GP path (Mandatory): Administrative Templates/Microsoft Edge/HTTP authentication
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: BasicAuthOverHttpEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: BasicAuthOverHttpEnabled
- Example value:

```
<false/>
```

Back to top

DisableAuthNegotiateCnameLookup

Disable CNAME lookup when negotiating Kerberos authentication

Supported versions:

- On Windows and macOS since 77 or later

Description

Determines whether the generated Kerberos SPN is based on the canonical DNS name (CNAME) or on the original name entered.

If you enable this policy, CNAME lookup is skipped and the server name (as entered) is used.

If you disable this policy or don't configure it, the canonical name of the server is used. This is determined through CNAME lookup.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DisableAuthNegotiateCnameLookup
- GP name: Disable CNAME lookup when negotiating Kerberos authentication
- GP path (Mandatory): Administrative Templates/Microsoft Edge/HTTP authentication
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DisableAuthNegotiateCnameLookup
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: DisableAuthNegotiateCnameLookup
- Example value:

```
<false/>
```

Back to top

EnableAuthNegotiatePort

Include non-standard port in Kerberos SPN

Supported versions:

- On Windows and macOS since 77 or later

Description

Specifies whether the generated Kerberos SPN should include a non-standard port.

If you enable this policy, and a user includes a non-standard port (a port other than 80 or 443) in a URL, that port is included in the generated Kerberos SPN.

If you don't configure or disable this policy, the generated Kerberos SPN won't include a port in any case.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EnableAuthNegotiatePort
- GP name: Include non-standard port in Kerberos SPN
- GP path (Mandatory): Administrative Templates/Microsoft Edge/HTTP authentication
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: EnableAuthNegotiatePort
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: EnableAuthNegotiatePort
- Example value:

```
<false/>
```

Back to top

NtlmV2Enabled

Control whether NTLMv2 authentication is enabled

Supported versions:

- On macOS since 77 or later

Description

Controls whether NTLMv2 is enabled.

All recent versions of Samba and Windows servers support NTLMv2. You should only disable NTLMv2 to address issues with backwards compatibility as it reduces the security of authentication.

If you don't configure this policy, NTLMv2 is enabled by default.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Mac information and settings

- Preference Key Name: NtlmV2Enabled
- Example value:

```
<true/>
```

Back to top

WindowsHelloForHTTPAuthEnabled

Windows Hello For HTTP Auth Enabled

Supported versions:

- On Windows since 90 or later

Description

Indicates if Windows Credential UI should be used to respond to NTLM and Negotiate authentication challenges.

If you disable this policy, a basic username and password prompt will be used to respond to NTLM and Negotiate challenges. If you enable or don't configure this policy, Windows Credential UI will be used.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WindowsHelloForHTTPAuthEnabled
- GP name: Windows Hello For HTTP Auth Enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/HTTP authentication
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/HTTP authentication
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: WindowsHelloForHTTPAuthEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

Identity and sign-in policies

Back to top

EdgeDefaultProfileEnabled

Default Profile Setting Enabled

Supported versions:

- On Windows since 101 or later

Description

Configuring this policy will let you set a default profile in Microsoft Edge to be used when opening the browser rather than the last profile used. This policy won't affect when "--profile-directory" parameter has been specified. Set the value to "Default" to refer to the default profile. The value is case sensitive. The value of the policy is the name of the profile (case sensitive) and can be configured with string that is the name of a specific profile. The value "Edge Kids Mode" and "Guest Profile" are considered not useful values because they not supposed to be a default profile. This policy won't impact the following scenarios:

1. Settings specified in "Profile preferences for sites" in "Profile preferences"
2. Links opening from Outlook and Teams.

The following statements are under the condition of not specify the "--profile-directory" and configured value is not "Edge Kids Mode" or "Guest Profile": If you enable this policy and configure it with a specific profile name and the specified profile can be found, Microsoft Edge will use the specified profile when launching and the setting of "Default profile for external link" is changed to the specified profile name and greyed out. If you enable this policy and configure it with a specific profile name but it can't be found, the policy will behave like it's never been set before. If you enable this policy, but don't configure or disable it, the policy will behave like it's never been set before.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EdgeDefaultProfileEnabled
- GP name: Default Profile Setting Enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Identity and sign-in
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: EdgeDefaultProfileEnabled
- Value Type: REG_SZ

Example value:

```
"Default"
```

Back to top

GuidedSwitchEnabled

Guided Switch Enabled

Supported versions:

- On Windows and macOS since 103 or later

Description

Allows Microsoft Edge to prompt the user to switch to the appropriate profile when Microsoft Edge detects that a link is a personal or work link.

If you enable this policy, you'll be prompted to switch to another account if the current profile doesn't work for the requesting link.

If you disable this policy, you won't be prompted to switch to another account when there's a profile and link mismatch.

If this policy isn't configured, guided switch is turned on by default. A user can override this value in the browser settings.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: GuidedSwitchEnabled
- GP name: Guided Switch Enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Identity and sign-in
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: GuidedSwitchEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: GuidedSwitchEnabled
- Example value:

```
<false/>
```

Back to top

ImplicitSignInEnabled

Enable implicit sign-in

Supported versions:

- On Windows since 93 or later

Description

Configure this policy to allow/disallow implicit sign-in.

If you have configured the BrowserSignin policy to 'Disable browser sign-in', this policy will not take any effect.

If you enable or don't configure this setting, implicit sign-in will be enabled, Edge will attempt to sign the user into their profile based on what and how they sign in to their OS.

If you disable this setting, implicit sign-in will be disabled.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ImplicitSignInEnabled
- GP name: Enable implicit sign-in
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Identity and sign-in
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ImplicitSignInEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

LinkedAccountEnabled

Enable the linked account feature

Supported versions:

- On Windows and macOS since 107 or later

Description

Microsoft Edge guides a user to the account management page where they can link a Microsoft Account (MSA) to an Azure Active Directory (Azure AD) account.

If you enable or don't configure this policy, linked account information will be shown on a flyout. When the Azure AD profile doesn't have a linked account it will show "Add account".

If you disable this policy, linked accounts will be turned off and no extra information will be shown.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: LinkedAccountEnabled
- GP name: Enable the linked account feature
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Identity and sign-in
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: LinkedAccountEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: LinkedAccountEnabled
- Example value:

```
<false/>
```

Back to top

OneAuthAuthenticationEnforced

OneAuth Authentication Flow Enforced for signin

Supported versions:

- On Windows since 93 or later

Description

This policy allows users to decide whether to use the OneAuth library for sign-in and token fetch in Microsoft Edge on Windows 10 RS3 and above.

If you disable or don't configure this policy, signin process will use Windows Account Manager. Microsoft Edge would be able to use accounts you logged in to Windows, Microsoft Office, or other Microsoft applications for login, without the needing of password. Or you can provide valid account and password to sign in, which will be stored in Windows Account Manager for future usage. You will be able to investigate all accounts stored in Windows Account Manager through Windows Settings -> Accounts -> Email and accounts page.

If you enable this policy, OneAuth authentication flow will be used for account signin. The OneAuth authentication flow has fewer dependencies and can work without Windows shell. The account you use would not be stored in the Email and accounts page.

This policy will only take effect on Windows 10 RS3 and above. On Windows 10 below RS3, OneAuth is used for authentication in Microsoft Edge by default.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: OneAuthAuthenticationEnforced
- GP name: OneAuth Authentication Flow Enforced for signin
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Identity and sign-in
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: OneAuthAuthenticationEnforced
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

OnlyOnPremisesImplicitSigninEnabled

Only on-premises account enabled for implicit sign-in

Supported versions:

- On Windows since 94 or later

Description

Configure this policy to decide whether only on-premises accounts are enabled for implicit sign-in.

If you enable this policy, only on-premises accounts will be enabled for implicit sign-in. Microsoft Edge won't attempt to implicitly sign in to MSA or AAD accounts. Upgrade from on-premises accounts to AAD accounts will be stopped as well.

If you disable or don't configure this policy, all accounts will be enabled for implicit sign-in.

This policy will only take effect when policy ConfigureOnPremisesAccountAutoSignIn is enabled and set to 'SignInAndMakeDomainAccountNonRemovable'.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: OnlyOnPremisesImplicitSigninEnabled
- GP name: Only on-premises account enabled for implicit sign-in
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Identity and sign-in
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge

- Path (Recommended): N/A
- Value Name: OnlyOnPremisesImplicitSigninEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

SignInCtaOnNtpEnabled

Enable sign in click to action dialog

Supported versions:

- On Windows and macOS since 99 or later

Description

Configure this policy to show sign in click to action dialog on New tab page.

If you enable or don't configure this policy, sign in click to action dialog is shown on New tab page.

If you disable this policy, sign in click to action dialog isn't shown on the New tab page.

Supported features:

- Can be mandatory: No
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SignInCtaOnNtpEnabled
- GP name: Enable sign in click to action dialog
- GP path (Mandatory): N/A
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Identity and sign-in
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): N/A
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: SignInCtaOnNtpEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: SignInCtaOnNtpEnabled
- Example value:

```
<true/>
```

Back to top

WAMAuthBelowWin10RS3Enabled

WAM for authentication below Windows 10 RS3 enabled

Supported versions:

- On Windows since 93 or later

Description

Configure this policy to decide whether WAM is used for authentication in Microsoft Edge on Windows 10 RS1 and RS2.

If you enable this setting, WAM will be used in the authentication flow on Windows 10 RS1 and RS2.

If you disable or don't configure this setting, OneAuth libraries will be used instead of WAM on Windows 10 RS1 and RS2.

Note that if this policy is enabled, then previous sign-in sessions (which used OneAuth by default) cannot be used. Please sign out of those profiles.

This policy will only take effect on Windows 10 RS1 and RS2. On Windows 10 RS3 and above, WAM is used for authentication in Microsoft Edge by default.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WAMAuthBelowWin10RS3Enabled
- GP name: WAM for authentication below Windows 10 RS3 enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Identity and sign-in
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: WAMAuthBelowWin10RS3Enabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

Kiosk Mode settings policies

Back to top

KioskAddressBarEditingEnabled

Configure address bar editing for kiosk mode public browsing experience

Supported versions:

- On Windows since 87 or later

Description

This policy only applies to Microsoft Edge kiosk mode while using the public browsing experience.

If you enable or don't configure this policy, users can change the URL in the address bar.

If you disable this policy, it prevents users from changing the URL in the address bar.

For detailed information on configuring kiosk Mode, see https://go.microsoft.com/fwlink/?linkid=2137578.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: KioskAddressBarEditingEnabled
- GP name: Configure address bar editing for kiosk mode public browsing experience
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Kiosk Mode settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: KioskAddressBarEditingEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

KioskDeleteDownloadsOnExit

Delete files downloaded as part of kiosk session when Microsoft Edge closes

Supported versions:

- On Windows since 87 or later

Description

This policy only applies to Microsoft Edge kiosk mode.

If you enable this policy, files downloaded as part of the kiosk session are deleted each time Microsoft Edge closes.

If you disable this policy or don't configure it, files downloaded as part of the kiosk session are not deleted when Microsoft Edge closes.

For detailed information on configuring kiosk Mode, see https://go.microsoft.com/fwlink/?linkid=2137578.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: KioskDeleteDownloadsOnExit
- GP name: Delete files downloaded as part of kiosk session when Microsoft Edge closes
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Kiosk Mode settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: KioskDeleteDownloadsOnExit
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

KioskSwipeGesturesEnabled

Swipe gestures in Microsoft Edge kiosk mode enabled

Supported versions:

- On Windows since 101 or later

Description

This policy only applies to Microsoft Edge kiosk mode.

If you enable this policy or don't configure it, swipe gestures will behave as expected.

If you disable this policy, the user will not be able to use swipe gestures (for example navigate forwards and backwards, refresh page).

For detailed information on configuring kiosk mode, see https://go.microsoft.com/fwlink/?linkid=2137578.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: KioskSwipeGesturesEnabled
- GP name: Swipe gestures in Microsoft Edge kiosk mode enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Kiosk Mode settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: KioskSwipeGesturesEnabled

- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

Manageability policies

Back to top

MAMEnabled

Mobile App Management Enabled

Supported versions:

- On Windows and macOS since 89 or later

Description

Allows the Microsoft Edge browser to retrieve policies from the Intune application management services and apply them to users' profiles.

If you enable this policy or don't configure it, Mobile App Management (MAM) Policies can be applied.

If you disable this policy, Microsoft Edge will not communicate with Intune to request MAM Policies.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: MAMEnabled
- GP name: Mobile App Management Enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Manageability
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: MAMEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: MAMEnabled
- Example value:

```
<false/>
```

Back to top

Native Messaging policies

Back to top

NativeMessagingAllowlist

Control which native messaging hosts users can use

Supported versions:

- On Windows and macOS since 77 or later

Description

Setting the policy specifies which native messaging hosts aren't subject to the deny list. A deny list value of * means all native messaging hosts are denied unless they're explicitly allowed.

All native messaging hosts are allowed by default. However, if a native messaging host is denied by policy, the admin can use the allow list to change that policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NativeMessagingAllowlist
- GP name: Control which native messaging hosts users can use
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Native Messaging
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\NativeMessagingAllowlist
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\NativeMessagingAllowlist\1 = "com.native.messaging.host.name1"
SOFTWARE\Policies\Microsoft\Edge\NativeMessagingAllowlist\2 = "com.native.messaging.host.name2"
```

Mac information and settings

- Preference Key Name: NativeMessagingAllowlist
- Example value:

```
<array>
  <string>com.native.messaging.host.name1</string>
  <string>com.native.messaging.host.name2</string>
</array>
```

Back to top

NativeMessagingBlocklist

Configure native messaging block list

Supported versions:

- On Windows and macOS since 77 or later

Description

Setting this policy specifies which native messaging hosts shouldn't be loaded. A deny list value of * means all native messaging hosts are denied unless they're explicitly allowed.

If you leave this policy unset , Microsoft Edge loads all installed native messaging hosts.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NativeMessagingBlocklist
- GP name: Configure native messaging block list
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Native Messaging
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\NativeMessagingBlocklist
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\NativeMessagingBlocklist\1 = "com.native.messaging.host.name1"
SOFTWARE\Policies\Microsoft\Edge\NativeMessagingBlocklist\2 = "com.native.messaging.host.name2"
```

Mac information and settings

- Preference Key Name: NativeMessagingBlocklist
- Example value:

```
<array>
  <string>com.native.messaging.host.name1</string>
  <string>com.native.messaging.host.name2</string>
</array>
```

Back to top

NativeMessagingUserLevelHosts

Allow user-level native messaging hosts (installed without admin permissions)

Supported versions:

- On Windows and macOS since 77 or later

Description

If you set this policy to Enabled or leave it unset, Microsoft Edge can use native messaging hosts installed at the user level.

If you set this policy to Disabled, Microsoft Edge can only use these hosts if they're installed at the system level.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NativeMessagingUserLevelHosts
- GP name: Allow user-level native messaging hosts (installed without admin permissions)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Native Messaging
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: NativeMessagingUserLevelHosts
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: NativeMessagingUserLevelHosts
- Example value:

```
<false/>
```

Back to top

Password manager and protection policies

Back to top

PasswordGeneratorEnabled

Allow users to get a strong password suggestion whenever they are creating an account online

Supported versions:

- On Windows and macOS since 93 or later

Description

Configures the Password Generator Settings toggle that enables/disables the feature for users.

If you enable or don't configure this policy, then Password Generator will offer users a strong and unique password suggestion (via a dropdown) on Signup and Change Password pages.

If you disable this policy, users will no longer see strong password suggestions on Signup or Change Password pages.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PasswordGeneratorEnabled
- GP name: Allow users to get a strong password suggestion whenever they are creating an account online
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Password manager and protection
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PasswordGeneratorEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: PasswordGeneratorEnabled
- Example value:

```
<false/>
```

Back to top

PasswordManagerBlocklist

Configure the list of domains for which the password manager UI (Save and Fill) will be disabled

Supported versions:

- On Windows and macOS since 99 or later

Description

Configure the list of domains where Microsoft Edge should disable the password manager. This means that Save and Fill workflows will be disabled, ensuring that passwords for those websites can't be saved or auto filled into web forms.

If you enable this policy, the password manager will be disabled for the specified set of domains.

If you disable or don't configure this policy, password manager will work as usual for all domains.

If you configure this policy, that is, add domains for which password manager is blocked, users can't change or override the behavior in Microsoft Edge. In addition, users can't use password manager for those URLs.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PasswordManagerBlocklist
- GP name: Configure the list of domains for which the password manager UI (Save and Fill) will be disabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Password manager and protection
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\PasswordManagerBlocklist
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\PasswordManagerBlocklist\1 = "https://contoso.com/"
SOFTWARE\Policies\Microsoft\Edge\PasswordManagerBlocklist\2 = "https://login.contoso.com"
```

Mac information and settings

- Preference Key Name: PasswordManagerBlocklist
- Example value:

```
<array>
  <string>https://contoso.com/</string>
  <string>https://login.contoso.com</string>
</array>
```

Back to top

PasswordManagerEnabled

Enable saving passwords to the password manager

Supported versions:

- On Windows and macOS since 77 or later

Description

Enable Microsoft Edge to save user passwords. The next time a user visits a site with a saved password, Microsoft Edge will enter the password automatically.

If you enable or don't configure this policy, users can save and add their passwords in Microsoft Edge.

If you disable this policy, users can't save and add new passwords, but they can still use previously saved passwords.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes

- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PasswordManagerEnabled
- GP name: Enable saving passwords to the password manager
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Password manager and protection
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Password manager and protection
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: PasswordManagerEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: PasswordManagerEnabled
- Example value:

```
<true/>
```

Back to top

PasswordManagerRestrictLengthEnabled

Restrict the length of passwords that can be saved in the Password Manager

Supported versions:

- On Windows and macOS since 104 or later

Description

Make Microsoft Edge restrict the length of usernames and/or passwords that can be saved in the Password Manager.

If you enable this policy, Microsoft Edge will not let the user save credentials with usernames and/or passwords longer than 256 characters.

If you disable or don't configure this policy, Microsoft Edge will let the user save credentials with arbitrarily long usernames and/or passwords.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PasswordManagerRestrictLengthEnabled
- GP name: Restrict the length of passwords that can be saved in the Password Manager
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Password manager and protection
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PasswordManagerRestrictLengthEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: PasswordManagerRestrictLengthEnabled
- Example value:

```
<true/>
```

Back to top

PasswordMonitorAllowed

Allow users to be alerted if their passwords are found to be unsafe

Supported versions:

- On Windows since 85 or later
- On macOS since 93 or later

Description

Allow Microsoft Edge to monitor user passwords.

If you enable this policy and a user consents to enabling the policy, the user will get alerted if any of their passwords stored in Microsoft Edge are found to be unsafe. Microsoft Edge will show an alert and this information will also be available in Settings > Passwords > Password Monitor.

If you disable this policy, users will not be asked for permission to enable this feature. Their passwords will not be scanned and they will not be alerted either.

If you enable or don't configure the policy, users can turn this feature on or off.

To learn more about how Microsoft Edge finds unsafe passwords see https://go.microsoft.com/fwlink/?linkid=2133833

Additional guidance:

This policy can be set as both Recommended as well as Mandatory, however with an important callout.

Mandatory enabled: Given that individual user consent is a pre-condition to enabling this feature for a given user, this policy does not have a Mandatory enabled setting. If the policy is set to Mandatory enabled, the UI in Settings will not change and the following error message will be displayed in edge://policy

Example Error state message: "This policy value is ignored because Password Monitor requires the consent of the individual user for it to be turned on. You can ask users in your Organization to go to Settings > Profile > Password and turn on the feature."

Recommended enabled: If the policy is set to Recommended enabled, the UI in Settings will remain in 'Off' state, but a briefcase icon will be made visible next to it with this description displayed on hover - "Your organization recommends a specific value for this setting and you have chosen a different value"

Mandatory and Recommended disabled: Both these states will work the normal way, with the usual captions being shown to users.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PasswordMonitorAllowed
- GP name: Allow users to be alerted if their passwords are found to be unsafe
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Password manager and protection
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Password manager and protection
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: PasswordMonitorAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: PasswordMonitorAllowed
- Example value:

```
<true/>
```

Back to top

PasswordProtectionChangePasswordURL

Configure the change password URL

Supported versions:

- On Windows and macOS since 77 or later

Description

Configures the change password URL (HTTP and HTTPS schemes only).

Password protection service will send users to this URL to change their password after seeing a warning in the browser.

If you enable this policy, then password protection service sends users to this URL to change their password.

If you disable this policy or don't configure it, then password protection service will not redirect users to a

change password URL.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management, or macOS instances that are that are managed via MDM or joined to a domain via MCX.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PasswordProtectionChangePasswordURL
- GP name: Configure the change password URL
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Password manager and protection
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PasswordProtectionChangePasswordURL
- Value Type: REG_SZ

Example value:

```
"https://contoso.com/change_password.html"
```

Mac information and settings

- Preference Key Name: PasswordProtectionChangePasswordURL
- Example value:

```
<string>https://contoso.com/change_password.html</string>
```

Back to top

PasswordProtectionLoginURLs

Configure the list of enterprise login URLs where the password protection service should capture salted hashes of a password

Supported versions:

- On Windows and macOS since 77 or later

Description

Configure the list of enterprise login URLs (HTTP and HTTPS schemes only) where Microsoft Edge should capture the salted hashes of passwords and use it for password reuse detection.

If you enable this policy, the password protection service captures fingerprints of passwords on the defined URLs.

If you disable this policy or don't configure it, no password fingerprints are captured.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management, or macOS instances that are that

are managed via MDM or joined to a domain via MCX.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PasswordProtectionLoginURLs
- GP name: Configure the list of enterprise login URLs where the password protection service should capture salted hashes of a password
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Password manager and protection
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\PasswordProtectionLoginURLs
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\PasswordProtectionLoginURLs\1 = "https://contoso.com/login.html"
SOFTWARE\Policies\Microsoft\Edge\PasswordProtectionLoginURLs\2 = "https://login.contoso.com"
```

Mac information and settings

- Preference Key Name: PasswordProtectionLoginURLs
- Example value:

```
<array>
  <string>https://contoso.com/login.html</string>
  <string>https://login.contoso.com</string>
</array>
```

Back to top

PasswordProtectionWarningTrigger

Configure password protection warning trigger

Supported versions:

- On Windows and macOS since 77 or later

Description

Allows you to control when to trigger password protection warning. Password protection alerts users when they reuse their protected password on potentially suspicious sites.

You can use the PasswordProtectionLoginURLs and PasswordProtectionChangePasswordURL policies to configure which passwords to protect.

Exemptions: Passwords for the sites listed in PasswordProtectionLoginURLs and PasswordProtectionChangePasswordURL, as well as for the sites listed in SmartScreenAllowListDomains, will not trigger a password-protection warning.

Set to 'PasswordProtectionWarningOff' to not show password protection warningss.

Set to 'PasswordProtectionWarningOnPasswordReuse' to show password protection warnings when the user reuses their protected password on a non-allowlisted site.

If you disable or don't configure this policy, then the warning trigger is not shown.

Policy options mapping:

- PasswordProtectionWarningOff (0) = Password protection warning is off
- PasswordProtectionWarningOnPasswordReuse (1) = Password protection warning is triggered by password reuse

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PasswordProtectionWarningTrigger
- GP name: Configure password protection warning trigger
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Password manager and protection
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PasswordProtectionWarningTrigger
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: PasswordProtectionWarningTrigger
- Example value:

```
<integer>1</integer>
```

Back to top

PasswordRevealEnabled

Enable Password reveal button

Supported versions:

- On Windows and macOS since 87 or later

Description

Lets you configure the default display of the browser password reveal button for password input fields on

websites.

If you enable or don't configure this policy, the browser user setting defaults to displaying the password reveal button.

If you disable this policy, the browser user setting won't display the password reveal button.

For accessibility, users can change the browser setting from the default policy.

This policy only affects the browser password reveal button, it doesn't affect websites' custom reveal buttons.

Supported features:

- Can be mandatory: No
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PasswordRevealEnabled
- GP name: Enable Password reveal button
- GP path (Mandatory): N/A
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Password manager and protection
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): N/A
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: PasswordRevealEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: PasswordRevealEnabled
- Example value:

```
<true/>
```

Back to top

PrimaryPasswordSetting

Configures a setting that asks users to enter their device password while using password autofill

Supported versions:

- On Windows and macOS since 93 or later

Description

The feature helps users add an additional layer of privacy to their online accounts by requiring device authentication (as a way of confirming the user's identity) before the saved password is auto-filled into a web form. This ensures that non-authorized persons can't use saved passwords for autofill.

This group policy configures the radio button selector that enables this feature for users. It also has a frequency

control where users can specify how often they would like to be prompted for authentication.

If you set this policy to 'Automatically', disable this policy, or don't configure this policy, autofill will not have any authentication flow.

If you set this policy to 'WithDevicePassword', users will have to enter their device password (or preferred mode of authentication under Windows) to prove their identity before their password is auto filled. Authentication modes include Windows Hello, PIN, face recognition, or fingerprint. The frequency for authentication prompt will be set to 'Always' by default. However, users can change it to the other option, which is 'Once every browsing session'.

If you set this policy to 'WithCustomPrimaryPassword', users will be asked to create their custom password and then to be redirected to Settings. After the custom password is set, users can authenticate themselves using the custom password and their passwords will get auto-filled after successful authentication. The frequency for authentication prompt will be set to 'Always' by default. However, users can change it to the other option, which is 'Once every browsing session'.

If you set this policy to 'AutofillOff', saved passwords will no longer be suggested for autofill.

Policy options mapping:

- Automatically (0) = Automatically
- WithDevicePassword (1) = With device password
- WithCustomPrimaryPassword (2) = With custom primary password
- AutofillOff (3) = Autofill off

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PrimaryPasswordSetting
- GP name: Configures a setting that asks users to enter their device password while using password autofill
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Password manager and protection
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PrimaryPasswordSetting
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: PrimaryPasswordSetting

- Example value:

```
<integer>0</integer>
```

Back to top

Performance policies

Back to top

EfficiencyMode

Configure when efficiency mode should become active

Supported versions:

- On Windows and macOS since 96 or later

Description

This policy setting lets you configure when efficiency mode will become active. By default, efficiency mode is set to 'BalancedSavings'. On devices with no battery, the default is for efficiency mode to never become active.

Individual sites may be blocked from participating in efficiency mode by configuring the policy SleepingTabsBlockedForUrls.

Set this policy to 'AlwaysActive' and efficiency mode will always be active.

Set this policy to 'NeverActive' and efficiency mode will never become active.

Set this policy to 'ActiveWhenUnplugged' and efficiency mode will become active when the device is unplugged.

Set this policy to 'ActiveWhenUnpluggedBatteryLow' and efficiency mode will become active when the device is unplugged and the battery is low.

Set this policy to 'BalancedSavings' and when the device is unplugged, efficiency mode will take moderate steps to save battery. When the device is unplugged and the battery is low, efficiency mode will take additional steps to save battery.

Set this policy to 'MaximumSavings' and when the device is unplugged or unplugged and the battery is low, efficiency mode takes additional steps to save battery.

If the device does not have a battery, efficiency mode will never become active in any mode other than 'AlwaysActive' unless the setting or EfficiencyModeEnabled policy is enabled.

This policy has no effect if the EfficiencyModeEnabled policy is disabled.

Learn more about efficiency mode: https://go.microsoft.com/fwlink/?linkid=2173921

Policy options mapping:

- AlwaysActive (0) = Efficiency mode is always active
- NeverActive (1) = Efficiency mode is never active
- ActiveWhenUnplugged (2) = Efficiency mode is active when the device is unplugged
- ActiveWhenUnpluggedBatteryLow (3) = Efficiency mode is active when the device is unplugged and the battery is low
- BalancedSavings (4) = When the device is unplugged, efficiency mode takes moderate steps to save battery. When the device is unplugged and the battery is low, efficiency mode takes additional steps to save battery.

- MaximumSavings (5) = When the device is unplugged or unplugged and the battery is low, efficiency mode takes additional steps to save battery.

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EfficiencyMode
- GP name: Configure when efficiency mode should become active
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Performance
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Performance
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: EfficiencyMode
- Value Type: REG_DWORD

Example value:

```
0x00000003
```

Mac information and settings

- Preference Key Name: EfficiencyMode
- Example value:

```
<integer>3</integer>
```

Back to top

EfficiencyModeEnabled

Efficiency mode enabled

Supported versions:

- On Windows and macOS since 106 or later

Description

Enables efficiency mode which helps extend battery life by saving computer resources. By default, efficiency mode is enabled for devices with a battery and disabled otherwise.

If you enable this policy, efficiency mode will become active according to the setting chosen by the user. You can configure the efficiency mode setting using the EfficiencyMode policy. If the device does not have a battery, efficiency mode will always be active.

If you disable this policy, efficiency mode will never become active. The EfficiencyMode and EfficiencyModeOnPowerEnabled policies will have no effect.

If you don't configure this policy, efficiency mode will be enabled for devices with a battery and disabled otherwise. Users can choose the efficiency mode option they want in edge://settings/system.

Learn more about efficiency mode: https://go.microsoft.com/fwlink/?linkid=2173921

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EfficiencyModeEnabled
- GP name: Efficiency mode enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Performance
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Performance
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: EfficiencyModeEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: EfficiencyModeEnabled
- Example value:

```
<true/>
```

Back to top

EfficiencyModeOnPowerEnabled

Enable efficiency mode when the device is connected to a power source

Supported versions:

- On Windows and macOS since 106 or later

Description

Allows efficiency mode to become active when the device is connected to a power source. On devices with no battery, this policy has no effect.

If you enable this policy, efficiency mode will become active when the device is connected to a power source.

If you disable or don't configure this policy, efficiency mode will never become active when the device is connected to a power source.

This policy has no effect if the EfficiencyModeEnabled policy is disabled.

Learn more about efficiency mode: https://go.microsoft.com/fwlink/?linkid=2173921

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EfficiencyModeOnPowerEnabled
- GP name: Enable efficiency mode when the device is connected to a power source
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Performance
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Performance
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: EfficiencyModeOnPowerEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: EfficiencyModeOnPowerEnabled
- Example value:

```
<true/>
```

Back to top

PerformanceDetectorEnabled

Performance Detector Enabled

Supported versions:

- On Windows and macOS since 107 or later

Description

The performance detector detects tab performance issues and recommends actions to fix the performance issues.

If you enable or don't configure this policy, performance detector is turned on.

If you disable this policy, performance detector is turned off.

The user can configure its behavior in edge://settings/system.

Learn more about performance detector: https://aka.ms/EdgePerformanceDetector

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PerformanceDetectorEnabled
- GP name: Performance Detector Enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Performance
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Performance
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: PerformanceDetectorEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: PerformanceDetectorEnabled
- Example value:

```
<true/>
```

Back to top

StartupBoostEnabled

Enable startup boost

Supported versions:

- On Windows since 88 or later

Description

Allows Microsoft Edge processes to start at OS sign-in and restart in background after the last browser window is closed.

If Microsoft Edge is running in background mode, the browser might not close when the last window is closed and the browser won't be restarted in background when the window closes. See the BackgroundModeEnabled policy for information about what happens after configuring Microsoft Edge background mode behavior.

If you enable this policy, startup boost is turned on.

If you disable this policy, startup boost is turned off.

If you don't configure this policy, startup boost may initially be off or on. The user can configure its behavior in edge://settings/system.

Learn more about startup boost: https://go.microsoft.com/fwlink/?linkid=2147018

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: StartupBoostEnabled
- GP name: Enable startup boost
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Performance
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Performance
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: StartupBoostEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

Permit or deny screen capture policies

Back to top

SameOriginTabCaptureAllowedByOrigins

Allow Same Origin Tab capture by these origins

Supported versions:

- On Windows and macOS since 97 or later

Description

Setting the policy lets you set a list of URL patterns that can capture tabs with their same Origin.

Leaving the policy unset means that sites will not be considered for an override at this scope of capture.

If a site matches a URL pattern in this policy, the following policies will not be considered: TabCaptureAllowedByOrigins, WindowCaptureAllowedByOrigins, ScreenCaptureAllowedByOrigins, ScreenCaptureAllowed.

For detailed information on valid url patterns, please see https://go.microsoft.com/fwlink/?linkid=2095322. This policy only matches based on origin, so any path in the URL pattern is ignored.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SameOriginTabCaptureAllowedByOrigins
- GP name: Allow Same Origin Tab capture by these origins

- GP path (Mandatory): Administrative Templates/Microsoft Edge/Permit or deny screen capture
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\SameOriginTabCaptureAllowedByOrigins
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\SameOriginTabCaptureAllowedByOrigins\1 = "https://www.example.com"
SOFTWARE\Policies\Microsoft\Edge\SameOriginTabCaptureAllowedByOrigins\2 = "[*.]example.edu"
```

Mac information and settings

- Preference Key Name: SameOriginTabCaptureAllowedByOrigins
- Example value:

```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

ScreenCaptureAllowedByOrigins

Allow Desktop, Window, and Tab capture by these origins

Supported versions:

- On Windows and macOS since 97 or later

Description

Setting the policy lets you set a list of URL patterns that can use Desktop, Window, and Tab Capture.

Leaving the policy unset means that sites will not be considered for an override at this scope of Capture.

This policy is not considered if a site matches a URL pattern in any of the following policies: WindowCaptureAllowedByOrigins, TabCaptureAllowedByOrigins, SameOriginTabCaptureAllowedByOrigins.

If a site matches a URL pattern in this policy, the ScreenCaptureAllowed will not be considered.

For detailed information on valid url patterns, please see https://go.microsoft.com/fwlink/?linkid=2095322. This policy only matches based on origin, so any path in the URL pattern is ignored.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ScreenCaptureAllowedByOrigins
- GP name: Allow Desktop, Window, and Tab capture by these origins

- GP path (Mandatory): Administrative Templates/Microsoft Edge/Permit or deny screen capture
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\ScreenCaptureAllowedByOrigins
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ScreenCaptureAllowedByOrigins\1 = "https://www.example.com"
SOFTWARE\Policies\Microsoft\Edge\ScreenCaptureAllowedByOrigins\2 = "[*.]example.edu"
```

Mac information and settings

- Preference Key Name: ScreenCaptureAllowedByOrigins
- Example value:

```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

TabCaptureAllowedByOrigins

Allow Tab capture by these origins

Supported versions:

- On Windows and macOS since 97 or later

Description

Setting the policy lets you set a list of URL patterns that can use Tab Capture.

Leaving the policy unset means that sites will not be considered for an override at this scope of capture.

This policy is not considered if a site matches a URL pattern in the SameOriginTabCaptureAllowedByOrigins policy.

If a site matches a URL pattern in this policy, the following policies will not be considered: WindowCaptureAllowedByOrigins, ScreenCaptureAllowedByOrigins, ScreenCaptureAllowed.

For detailed information on valid url patterns, please see https://go.microsoft.com/fwlink/?linkid=2095322. This policy only matches based on origin, so any path in the URL pattern is ignored.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: TabCaptureAllowedByOrigins
- GP name: Allow Tab capture by these origins

- GP path (Mandatory): Administrative Templates/Microsoft Edge/Permit or deny screen capture
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\TabCaptureAllowedByOrigins
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\TabCaptureAllowedByOrigins\1 = "https://www.example.com"
SOFTWARE\Policies\Microsoft\Edge\TabCaptureAllowedByOrigins\2 = "[*.]example.edu"
```

Mac information and settings

- Preference Key Name: TabCaptureAllowedByOrigins
- Example value:

```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

WindowCaptureAllowedByOrigins

Allow Window and Tab capture by these origins

Supported versions:

- On Windows and macOS since 97 or later

Description

Setting the policy lets you set a list of URL patterns that can use Window and Tab Capture.

Leaving the policy unset means that sites will not be considered for an override at this scope of Capture.

This policy is not considered if a site matches a URL pattern in any of the following policies: TabCaptureAllowedByOrigins, SameOriginTabCaptureAllowedByOrigins.

If a site matches a URL pattern in this policy, the following policies will not be considered: ScreenCaptureAllowedByOrigins, ScreenCaptureAllowed.

For detailed information on valid url patterns, please see https://go.microsoft.com/fwlink/?linkid=2095322. This policy only matches based on origin, so any path in the URL pattern is ignored.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WindowCaptureAllowedByOrigins

- GP name: Allow Window and Tab capture by these origins
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Permit or deny screen capture
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\WindowCaptureAllowedByOrigins
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\WindowCaptureAllowedByOrigins\1 = "https://www.example.com"
SOFTWARE\Policies\Microsoft\Edge\WindowCaptureAllowedByOrigins\2 = "[*.]example.edu"
```

Mac information and settings

- Preference Key Name: WindowCaptureAllowedByOrigins
- Example value:

```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

Printing policies

Back to top

DefaultPrinterSelection

Default printer selection rules

Supported versions:

- On Windows and macOS since 77 or later

Description

Overrides Microsoft Edge default printer selection rules. This policy determines the rules for selecting the default printer in Microsoft Edge, which happens the first time a user tries to print a page.

When this policy is set, Microsoft Edge tries to find a printer that matches all of the specified attributes and uses it as default printer. If there are multiple printers that meet the criteria, the first printer that matches is used.

If you don't configure this policy or no matching printers are found within the timeout, the printer defaults to the built-in PDF printer or no printer, if the PDF printer isn't available.

The value is parsed as a JSON object, conforming to the following schema: { "type": "object", "properties": { "idPattern": { "description": "Regular expression to match printer id.", "type": "string" }, "namePattern": { "description": "Regular expression to match printer display name.", "type": "string" } } }

Omitting a field means all values match; for example, if you don't specify connectivity Print Preview starts discovering all kinds of local printers. Regular expression patterns must follow the JavaScript RegExp syntax and matches are case sensitive.

Supported features:

- Can be mandatory: Yes

- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultPrinterSelection
- GP name: Default printer selection rules
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Printing
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefaultPrinterSelection
- Value Type: REG_SZ

Example value:

```
"{ \"idPattern\": \".*public\", \"namePattern\": \".*Color\" }"
```

Mac information and settings

- Preference Key Name: DefaultPrinterSelection
- Example value:

```
<string>{ "idPattern": ".*public", "namePattern": ".*Color" }</string>
```

Back to top

PrintHeaderFooter

Print headers and footers

Supported versions:

- On Windows and macOS since 77 or later

Description

Force 'headers and footers' to be on or off in the printing dialog.

If you don't configure this policy, users can decide whether to print headers and footers.

If you disable this policy, users can't print headers and footers.

If you enable this policy, users always print headers and footers.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PrintHeaderFooter

- GP name: Print headers and footers
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Printing
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Printing
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: PrintHeaderFooter
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: PrintHeaderFooter
- Example value:

```
<false/>
```

Back to top

PrintPdfAsImageDefault

Print PDF as Image Default

Supported versions:

- On Windows and macOS since 106 or later

Description

Controls if Microsoft Edge makes the Print as image option the default when printing PDFs.

If you enable this policy, Microsoft Edge will default to setting the Print as image option in the Print Preview when printing a PDF.

If you disable or don't configure this policy, Microsoft Edge will not default to setting the Print as image option in the Print Preview when printing a PDF.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PrintPdfAsImageDefault
- GP name: Print PDF as Image Default
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Printing
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge

- Path (Recommended): N/A
- Value Name: PrintPdfAsImageDefault
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: PrintPdfAsImageDefault
- Example value:

```
<true/>
```

Back to top

PrintPostScriptMode

Print PostScript Mode

Supported versions:

- On Windows since 96 or later

Description

Controls how Microsoft Edge prints on Microsoft Windows.

Printing to a PostScript printer on Microsoft Windows different PostScript generation methods can affect printing performance.

If you set this policy to Default, Microsoft Edge will use a set of default options when generating PostScript. For text in particular, text will always be rendered using Type 3 fonts.

If you set this policy to Type42, Microsoft Edge will render text using Type 42 fonts if possible. This should increase printing speed for some PostScript printers.

If you don't configure this policy, Microsoft Edge will be in Default mode.

Policy options mapping:

- Default (0) = Default
- Type42 (1) = Type42

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PrintPostScriptMode
- GP name: Print PostScript Mode
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Printing
- GP path (Recommended): N/A

- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PrintPostScriptMode
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

PrintPreviewUseSystemDefaultPrinter

Set the system default printer as the default printer

Supported versions:

- On Windows and macOS since 77 or later

Description

Tells Microsoft Edge to use the system default printer as the default choice in Print Preview instead of the most recently used printer.

If you disable this policy or don't configure it, Print Preview uses the most recently used printer as the default destination choice.

If you enable this policy, Print Preview uses the OS system default printer as the default destination choice.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PrintPreviewUseSystemDefaultPrinter
- GP name: Set the system default printer as the default printer
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Printing
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Printing
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: PrintPreviewUseSystemDefaultPrinter
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: PrintPreviewUseSystemDefaultPrinter

- Example value:

```
<false/>
```

Back to top

PrintRasterizationMode

Print Rasterization Mode

Supported versions:

- On Windows since 90 or later

Description

Controls how Microsoft Edge prints on Windows.

When printing to a non-PostScript printer on Windows, sometimes print jobs need to be rasterized to print correctly.

If you set this policy to 'Full' or don't configure it, Microsoft Edge will do full page rasterization if necessary.

If you set this policy to 'Fast', Microsoft Edge will reduce the amount of rasterization which can help reduce print job sizes and increase printing speed.

Policy options mapping:

- Full (0) = Full page rasterization
- Fast (1) = Avoid rasterization if possible

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PrintRasterizationMode
- GP name: Print Rasterization Mode
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Printing
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PrintRasterizationMode
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

PrintRasterizePdfDpi

Print Rasterize PDF DPI

Supported versions:

- On Windows and macOS since 96 or later

Description

Controls print image resolution when Microsoft Edge prints PDFs with rasterization.

When printing a PDF using the Print to image option, it can be beneficial to specify a print resolution other than a device's printer setting or the PDF default. A high resolution will significantly increase the processing and printing time while a low resolution can lead to poor imaging quality.

If you set this policy, it allows a particular resolution to be specified for use when rasterizing PDFs for printing.

If you set this policy to zero or don't configure it, the system default resolution will be used during rasterization of page images.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PrintRasterizePdfDpi
- GP name: Print Rasterize PDF DPI
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Printing
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PrintRasterizePdfDpi
- Value Type: REG_DWORD

Example value:

```
0x0000012c
```

Mac information and settings

- Preference Key Name: PrintRasterizePdfDpi
- Example value:

```
<integer>300</integer>
```

Back to top

PrintStickySettings

Print preview sticky settings

Supported versions:

- On Windows and macOS since 98 or later

Description

Specifies whether print preview should apply last used settings for Microsoft Edge PDF and webpages.

If you set this policy to 'EnableAll' or don't configure it, Microsoft Edge applies the last used print preview settings for both PDF and webpages.

If you set this policy to 'DisableAll', Microsoft Edge doesn't apply the last used print preview settings for both PDF and webpages.

If you set this policy to 'DisablePdf', Microsoft Edge doesn't apply the last used print preview settings for PDF printing and retains it for webpages.

If you set this policy to 'DisableWebpage', Microsoft Edge doesn't apply the last used print preview settings for webpage printing and retain it for PDF.

This policy is only available if you enable or don't configure the PrintingEnabled policy.

Policy options mapping:

- EnableAll (0) = Enable sticky settings for PDF and Webpages
- DisableAll (1) = Disable sticky settings for PDF and Webpages
- DisablePdf (2) = Disable sticky settings for PDF
- DisableWebpage (3) = Disable sticky settings for Webpages

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PrintStickySettings
- GP name: Print preview sticky settings
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Printing
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PrintStickySettings
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: PrintStickySettings
- Example value:

```
<integer>1</integer>
```

Back to top

PrinterTypeDenyList

Disable printer types on the deny list

Supported versions:

- On Windows and macOS since 88 or later

Description

The printer types on the deny list won't be discovered or have their capabilities fetched.

Placing all printer types on the deny list effectively disables printing, because there's no print destination for documents.

If you don't configure this policy, or the printer list is empty, all printer types are discoverable.

Printer destinations include extension printers and local printers. Extension printers are also known as print provider destinations, and include any destination that belongs to a Microsoft Edge extension. Local printers are also known as native printing destinations, and include destinations available to the local machine and shared network printers.

In Microsoft version 93 or later, if you set this policy to 'pdf' it also disables the 'save as Pdf' option from the right click context menu.

In Microsoft version 103 or later, if you set this policy to 'onedrive' it also disables the 'save as Pdf (OneDrive)' option from print preview.

Policy options mapping:

- privet (privet) = Zeroconf-based (mDNS + DNS-SD) protocol destinations
- extension (extension) = Extension-based destinations
- pdf (pdf) = The 'Save as PDF' destination. (93 or later, also disables from context menu)
- local (local) = Local printer destinations
- onedrive (onedrive) = Save as PDF (OneDrive) printer destinations. (103 or later)

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PrinterTypeDenyList
- GP name: Disable printer types on the deny list
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Printing
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\PrinterTypeDenyList
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\PrinterTypeDenyList\1 = "local"
SOFTWARE\Policies\Microsoft\Edge\PrinterTypeDenyList\2 = "privet"
```

Mac information and settings

- Preference Key Name: PrinterTypeDenyList
- Example value:

```
<array>
  <string>local</string>
  <string>privet</string>
</array>
```

Back to top

PrintingAllowedBackgroundGraphicsModes

Restrict background graphics printing mode

Supported versions:

- On Windows and macOS since 89 or later

Description

Restricts background graphics printing mode. If this policy isn't set there's no restriction on printing background graphics.

Policy options mapping:

- any (any) = Allow printing with and without background graphics
- enabled (enabled) = Allow printing only with background graphics
- disabled (disabled) = Allow printing only without background graphics

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PrintingAllowedBackgroundGraphicsModes
- GP name: Restrict background graphics printing mode
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Printing
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PrintingAllowedBackgroundGraphicsModes
- Value Type: REG_SZ

Example value:

```
"enabled"
```

Mac information and settings

- Preference Key Name: PrintingAllowedBackgroundGraphicsModes
- Example value:

```
<string>enabled</string>
```

Back to top

PrintingBackgroundGraphicsDefault

Default background graphics printing mode

Supported versions:

- On Windows and macOS since 89 or later

Description

Overrides the last used setting for printing background graphics. If you enable this setting, background graphics printing is enabled. If you disable this setting, background graphics printing is disabled.

Policy options mapping:

- enabled (enabled) = Enable background graphics printing mode by default
- disabled (disabled) = Disable background graphics printing mode by default

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PrintingBackgroundGraphicsDefault
- GP name: Default background graphics printing mode
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Printing
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PrintingBackgroundGraphicsDefault
- Value Type: REG_SZ

Example value:

```
"enabled"
```

Mac information and settings

- Preference Key Name: PrintingBackgroundGraphicsDefault
- Example value:

```
<string>enabled</string>
```

Back to top

PrintingEnabled

Enable printing

Supported versions:

- On Windows and macOS since 77 or later

Description

Enables printing in Microsoft Edge and prevents users from changing this setting.

If you enable this policy or don't configure it, users can print.

If you disable this policy, users can't print from Microsoft Edge. Printing is disabled in the wrench menu, extensions, JavaScript applications, and so on. Users can still print from plug-ins that bypass Microsoft Edge while printing. For example, certain Adobe Flash applications have the print option in their context menu, which isn't covered by this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PrintingEnabled
- GP name: Enable printing
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Printing
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PrintingEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: PrintingEnabled
- Example value:

```
<true/>
```

Back to top

PrintingPaperSizeDefault

Default printing page size

Supported versions:

- On Windows and macOS since 86 or later

Description

Overrides default printing page size.

name should contain one of the listed formats or 'custom' if required paper size is not in the list. If 'custom' value is provided custom_size property should be specified. It describes the desired height and width in micrometers. Otherwise custom_size property shouldn't be specified. Policy that violates these rules is ignored.

If the page size is unavailable on the printer chosen by the user this policy is ignored.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Dictionary

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PrintingPaperSizeDefault
- GP name: Default printing page size
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Printing
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PrintingPaperSizeDefault
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\PrintingPaperSizeDefault = {
  "custom_size": {
    "height": 297000,
    "width": 210000
  },
  "name": "custom"
}
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\PrintingPaperSizeDefault = {"custom_size": {"height": 297000, "width":
210000}, "name": "custom"}
```

Mac information and settings

- Preference Key Name: PrintingPaperSizeDefault

- Example value:

```
<key>PrintingPaperSizeDefault</key>
<dict>
  <key>custom_size</key>
  <dict>
    <key>height</key>
    <integer>297000</integer>
    <key>width</key>
    <integer>210000</integer>
  </dict>
  <key>name</key>
  <string>custom</string>
</dict>
```

Back to top

PrintingWebpageLayout

Sets layout for printing

Supported versions:

- On Windows and macOS since 93 or later

Description

Configuring this policy sets the layout for printing webpages.

If you disable or don't configure this policy, users can decide whether to print webpages in Portrait or Landscape layout.

If you enable this policy, the selected option is set as the layout option.

Policy options mapping:

- portrait (0) = Sets layout option as portrait
- landscape (1) = Sets layout option as landscape

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PrintingWebpageLayout
- GP name: Sets layout for printing
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Printing
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Printing
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: PrintingWebpageLayout

- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: PrintingWebpageLayout
- Example value:

```
<integer>0</integer>
```

Back to top

UseSystemPrintDialog

Print using system print dialog

Supported versions:

- On Windows and macOS since 77 or later

Description

Shows the system print dialog instead of print preview.

If you enable this policy, Microsoft Edge opens the system print dialog instead of the built-in print preview when a user prints a page.

If you don't configure or disable this policy, print commands trigger the Microsoft Edge print preview screen.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: UseSystemPrintDialog
- GP name: Print using system print dialog
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Printing
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: UseSystemPrintDialog
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: UseSystemPrintDialog
- Example value:

```
<false/>
```

Back to top

Private Network Request Settings policies

Back to top

InsecurePrivateNetworkRequestsAllowed

Specifies whether to allow insecure websites to make requests to more-private network endpoints

Supported versions:

- On Windows and macOS since 92 or later

Description

Controls whether insecure websites are allowed to make requests to more-private network endpoints.

This policy relates to the Private Network Access specification. See https://wicg.github.io/private-network-access/ for more details.

A network endpoint is more private than another if:

1. Its IP address is localhost and the other is not.
2. Its IP address is private and the other is public. In the future, depending on spec evolution, this policy might apply to all cross-origin requests directed at private IPs or localhost.

A website is deemed secure if it meets the definition of a secure context in https://developer.mozilla.org/en-US/docs/Web/Security/Secure_Contexts. Otherwise, it will be treated as an insecure context.

When this policy is either not set or set to false, the default behavior for requests from insecure contexts to more-private network endpoints will depend on the user's personal configuration for the BlockInsecurePrivateNetworkRequests feature, which may be set by a field trial or on the command line.

When this policy is set to true, insecure websites are allowed to make requests to any network endpoint, subject to other cross-origin checks.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InsecurePrivateNetworkRequestsAllowed
- GP name: Specifies whether to allow insecure websites to make requests to more-private network endpoints
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Private Network Request Settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InsecurePrivateNetworkRequestsAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: InsecurePrivateNetworkRequestsAllowed
- Example value:

```
<false/>
```

Back to top

InsecurePrivateNetworkRequestsAllowedForUrls

Allow the listed sites to make requests to more-private network endpoints from insecure contexts

Supported versions:

- On Windows and macOS since 92 or later

Description

List of URL patterns. Private network requests initiated from insecure websites served by matching origins are allowed.

If this policy is not set, this policy behaves as if set to the empty list.

For origins not covered by the patterns specified here, the global default value will be used either from the InsecurePrivateNetworkRequestsAllowed policy, if it is set, or the user's personal configuration otherwise.

Note that this policy only affects insecure origins, so secure origins (e.g. https://example.com) included in this list will be ignored.

For detailed information on valid URL patterns, see Filter format for URL list-based policies.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InsecurePrivateNetworkRequestsAllowedForUrls
- GP name: Allow the listed sites to make requests to more-private network endpoints from insecure contexts
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Private Network Request Settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\InsecurePrivateNetworkRequestsAllowedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\InsecurePrivateNetworkRequestsAllowedForUrls\1 =
"http://www.example.com:8080"
SOFTWARE\Policies\Microsoft\Edge\InsecurePrivateNetworkRequestsAllowedForUrls\2 = "[*.]example.edu"
```

Mac information and settings

- Preference Key Name: InsecurePrivateNetworkRequestsAllowedForUrls
- Example value:

```
<array>
  <string>http://www.example.com:8080</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

Proxy server policies

Back to top

ProxyBypassList

Configure proxy bypass rules (deprecated)

> DEPRECATED: This policy is deprecated. It is currently supported but will become obsolete in a future release.

Supported versions:

- On Windows and macOS since 77 or later

Description

This policy is deprecated, use ProxySettings instead. It won't work in Microsoft Edge version 91.

Defines a list of hosts for which Microsoft Edge bypasses any proxy.

This policy is applied only if the ProxySettings policy isn't specified and you have selected either fixed_servers or pac_script in the ProxyMode policy. If you selected any other mode for configuring proxy policies, don't enable or configure this policy.

If you enable this policy, you can create a list of hosts for which Microsoft Edge doesn't use a proxy.

If you don't configure this policy, no list of hosts is created for which Microsoft Edge bypasses a proxy. Leave this policy unconfigured if you've specified any other method for setting proxy policies.

For more detailed examples go to https://go.microsoft.com/fwlink/?linkid=2094936.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ProxyBypassList
- GP name: Configure proxy bypass rules (deprecated)

- GP path (Mandatory): Administrative Templates/Microsoft Edge/Proxy server
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ProxyBypassList
- Value Type: REG_SZ

Example value:

```
"https://www.contoso.com, https://www.fabrikam.com"
```

Mac information and settings

- Preference Key Name: ProxyBypassList
- Example value:

```
<string>https://www.contoso.com, https://www.fabrikam.com</string>
```

Back to top

ProxyMode

Configure proxy server settings (deprecated)

> DEPRECATED: This policy is deprecated. It is currently supported but will become obsolete in a future release.

Supported versions:

- On Windows and macOS since 77 or later

Description

This policy is deprecated, use ProxySettings instead. It won't work in Microsoft Edge version 91.

If you set this policy to Enabled you can specify the proxy server Microsoft Edge uses and prevents users from changing proxy settings. Microsoft Edge ignores all proxy-related options specified from the command line. The policy is only applied if the ProxySettings policy isn't specified.

Other options are ignored if you choose one of the following options:

- direct = Never use a proxy server and always connect directly
- system = Use system proxy settings
- auto_detect = Auto detect the proxy server

If you choose to use:

- fixed_servers = Fixed proxy servers. You can specify further options with ProxyServer and ProxyBypassList.
- pac_script = A .pac proxy script. Use ProxyPacUrl to set the URL to a proxy .pac file.

For detailed examples, go to https://go.microsoft.com/fwlink/?linkid=2094936.

If you don't configure this policy, users can choose their own proxy settings.

Policy options mapping:

- ProxyDisabled (direct) = Never use a proxy

- ProxyAutoDetect (auto_detect) = Auto detect proxy settings
- ProxyPacScript (pac_script) = Use a .pac proxy script
- ProxyFixedServers (fixed_servers) = Use fixed proxy servers
- ProxyUseSystem (system) = Use system proxy settings

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ProxyMode
- GP name: Configure proxy server settings (deprecated)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Proxy server
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ProxyMode
- Value Type: REG_SZ

Example value:

```
"direct"
```

Mac information and settings

- Preference Key Name: ProxyMode
- Example value:

```
<string>direct</string>
```

Back to top

ProxyPacUrl

Set the proxy .pac file URL (deprecated)

> DEPRECATED: This policy is deprecated. It is currently supported but will become obsolete in a future release.

Supported versions:

- On Windows and macOS since 77 or later

Description

This policy is deprecated, use ProxySettings instead. It won't work in Microsoft Edge version 91.

Specifies the URL for a proxy auto-config (PAC) file.

This policy is applied only if the ProxySettings policy isn't specified and you have selected pac_script in the ProxyMode policy. If you selected any other mode for configuring proxy policies, don't enable or configure this policy.

If you enable this policy, you can specify the URL for a PAC file, which defines how the browser automatically chooses the appropriate proxy server for fetching a particular website.

If you disable or don't configure this policy, no PAC file is specified. Leave this policy unconfigured if you've specified any other method for setting proxy policies.

For detailed examples, see https://go.microsoft.com/fwlink/?linkid=2094936.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ProxyPacUrl
- GP name: Set the proxy .pac file URL (deprecated)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Proxy server
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ProxyPacUrl
- Value Type: REG_SZ

Example value:

```
"https://internal.contoso.com/example.pac"
```

Mac information and settings

- Preference Key Name: ProxyPacUrl
- Example value:

```
<string>https://internal.contoso.com/example.pac</string>
```

Back to top

ProxyServer

Configure address or URL of proxy server (deprecated)

> DEPRECATED: This policy is deprecated. It is currently supported but will become obsolete in a future release.

Supported versions:

- On Windows and macOS since 77 or later

Description

This policy is deprecated, use ProxySettings instead. It won't work in Microsoft Edge version 91.

Specifies the URL of the proxy server.

This policy is applied only if the ProxySettings policy isn't specified and you have selected fixed_servers in the ProxyMode policy. If you selected any other mode for configuring proxy policies, don't enable or configure this policy.

If you enable this policy, the proxy server configured by this policy will be used for all URLs.

If you disable or don't configure this policy, users can choose their own proxy settings while in this proxy mode. Leave this policy unconfigured if you've specified any other method for setting proxy policies.

For more options and detailed examples, see https://go.microsoft.com/fwlink/?linkid=2094936.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ProxyServer
- GP name: Configure address or URL of proxy server (deprecated)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Proxy server
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ProxyServer
- Value Type: REG_SZ

Example value:

```
"123.123.123.123:8080"
```

Mac information and settings

- Preference Key Name: ProxyServer
- Example value:

```
<string>123.123.123.123:8080</string>
```

Back to top

ProxySettings

Proxy settings

Supported versions:

- On Windows and macOS since 77 or later

Description

Configures the proxy settings for Microsoft Edge.

If you enable this policy, Microsoft Edge ignores all proxy-related options specified from the command line.

If you don't configure this policy, users can choose their own proxy settings.

This policy overrides the following individual policies:

ProxyMode ProxyPacUrl ProxyServer ProxyBypassList

Setting the ProxySettings policy accepts the following fields:

- ProxyMode, which lets you specify the proxy server used by Microsoft Edge and prevents users from changing proxy settings
- ProxyPacUrl, a URL to a proxy .pac file
- ProxyPacMandatory, a boolean flag which prevents the network stack from falling back to direct connections with invalid or unavailable PAC script
- ProxyServer, a URL for the proxy server
- ProxyBypassList, a list of proxy hosts that Microsoft Edge bypasses

For ProxyMode, if you choose the value:

- direct, a proxy is never used and all other fields are ignored.
- system, the systems's proxy is used and all other fields are ignored.
- auto_detect, all other fields are ignored.
- fixed_servers, the ProxyServer and ProxyBypassList fields are used.
- pac_script, the ProxyPacUrl, ProxyPacMandatory and ProxyBypassList fields are used.

For more detailed examples go to https://go.microsoft.com/fwlink/?linkid=2094936.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Dictionary

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ProxySettings
- GP name: Proxy settings
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Proxy server
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ProxySettings
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ProxySettings = {
  "ProxyBypassList": "https://www.example1.com,https://www.example2.com,https://internalsite/",
  "ProxyMode": "pac_script",
  "ProxyPacMandatory": false,
  "ProxyPacUrl": "https://internal.site/example.pac",
  "ProxyServer": "123.123.123.123:8080"
}
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\ProxySettings = {"ProxyBypassList":
"https://www.example1.com,https://www.example2.com,https://internalsite/", "ProxyMode": "pac_script",
"ProxyPacMandatory": false, "ProxyPacUrl": "https://internal.site/example.pac", "ProxyServer":
"123.123.123.123:8080"}
```

Mac information and settings

- Preference Key Name: ProxySettings
- Example value:

```
<key>ProxySettings</key>
<dict>
  <key>ProxyBypassList</key>
  <string>https://www.example1.com,https://www.example2.com,https://internalsite/</string>
  <key>ProxyMode</key>
  <string>pac_script</string>
  <key>ProxyPacMandatory</key>
  <false/>
  <key>ProxyPacUrl</key>
  <string>https://internal.site/example.pac</string>
  <key>ProxyServer</key>
  <string>123.123.123.123:8080</string>
</dict>
```

Back to top

Sleeping tabs settings policies

Back to top

SleepingTabsBlockedForUrls

Block sleeping tabs on specific sites

Supported versions:

- On Windows and macOS since 88 or later

Description

Define a list of sites, based on URL patterns, that are not allowed to be put to sleep by sleeping tabs. Sites in this list are also excluded from other performance optimizations like efficiency mode and tab discard.

If the policy SleepingTabsEnabled is disabled, this list is not used and no sites will be put to sleep automatically.

If you don't configure this policy, all sites will be eligible to be put to sleep unless the user's personal configuration blocks them.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SleepingTabsBlockedForUrls
- GP name: Block sleeping tabs on specific sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Sleeping tabs settings
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Sleeping tabs settings
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\SleepingTabsBlockedForUrls
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended\SleepingTabsBlockedForUrls
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\SleepingTabsBlockedForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\SleepingTabsBlockedForUrls\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: SleepingTabsBlockedForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

SleepingTabsEnabled

Configure sleeping tabs

Supported versions:

- On Windows and macOS since 88 or later

Description

This policy setting lets you configure whether to turn on sleeping tabs. Sleeping tabs reduces CPU, battery, and memory usage by putting idle background tabs to sleep. Microsoft Edge uses heuristics to avoid putting tabs to sleep that do useful work in the background, such as display notifications, play sound, and stream video. By default, sleeping tabs is turned on.

Individual sites may be blocked from being put to sleep by configuring the policy SleepingTabsBlockedForUrls.

If you enable this setting, sleeping tabs is turned on.

If you disable this setting, sleeping tabs is turned off.

If you don't configure this setting, users can choose whether to use sleeping tabs.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SleepingTabsEnabled
- GP name: Configure sleeping tabs
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Sleeping tabs settings
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Sleeping tabs settings
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: SleepingTabsEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: SleepingTabsEnabled
- Example value:

```
<true/>
```

Back to top

SleepingTabsTimeout

Set the background tab inactivity timeout for sleeping tabs

Supported versions:

- On Windows and macOS since 88 or later

Description

This policy setting lets you configure the timeout, in seconds, after which inactive background tabs will be automatically put to sleep if sleeping tabs is enabled. By default, this timeout is 7,200 seconds (2 hours).

Tabs are only put to sleep automatically when the policy SleepingTabsEnabled is enabled or is not configured and the user has enabled the sleeping tabs setting.

If you don't configure this policy, users can choose the timeout value.

Policy options mapping:

- 30Seconds (30) = 30 seconds of inactivity
- 5Minutes (300) = 5 minutes of inactivity
- 15Minutes (900) = 15 minutes of inactivity
- 30Minutes (1800) = 30 minutes of inactivity
- 1Hour (3600) = 1 hour of inactivity
- 2Hours (7200) = 2 hours of inactivity

- 3Hours (10800) = 3 hours of inactivity
- 6Hours (21600) = 6 hours of inactivity
- 12Hours (43200) = 12 hours of inactivity

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SleepingTabsTimeout
- GP name: Set the background tab inactivity timeout for sleeping tabs
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Sleeping tabs settings
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Sleeping tabs settings
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: SleepingTabsTimeout
- Value Type: REG_DWORD

Example value:

```
0x00000384
```

Mac information and settings

- Preference Key Name: SleepingTabsTimeout
- Example value:

```
<integer>900</integer>
```

Back to top

SmartScreen settings policies

Back to top

NewSmartScreenLibraryEnabled

Enable new SmartScreen library (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 107.

Supported versions:

- On Windows and macOS since 95, until 107

Description

This policy doesn't work because it was only intended to be a short-term mechanism to support the update to a new SmartScreen client.

Allows the Microsoft Edge browser to load the new SmartScreen library (libSmartScreenN) for any SmartScreen checks on site URLs or application downloads.

If you enable or don't configure this policy, Microsoft Edge will use the new SmartScreen library (libSmartScreenN).

If you disable this policy, Microsoft Edge will use the old SmartScreen library (libSmartScreen).

Before Microsoft Edge version 103, if you don't configure this policy, Microsoft Edge will use the old SmartScreen library (libSmartScreen).

This policy is only available on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management. This also includes macOS instances that are that are managed via MDM or joined to a domain via MCX.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NewSmartScreenLibraryEnabled
- GP name: Enable new SmartScreen library (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/SmartScreen settings
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/SmartScreen settings
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: NewSmartScreenLibraryEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: NewSmartScreenLibraryEnabled
- Example value:

```
<true/>
```

Back to top

PreventSmartScreenPromptOverride

Prevent bypassing Microsoft Defender SmartScreen prompts for sites

Supported versions:

- On Windows and macOS since 77 or later

Description

This policy setting lets you decide whether users can override the Microsoft Defender SmartScreen warnings about potentially malicious websites.

If you enable this setting, users can't ignore Microsoft Defender SmartScreen warnings and they are blocked from continuing to the site.

If you disable or don't configure this setting, users can ignore Microsoft Defender SmartScreen warnings and continue to the site.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management, or macOS instances that are that are managed via MDM or joined to a domain via MCX.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PreventSmartScreenPromptOverride
- GP name: Prevent bypassing Microsoft Defender SmartScreen prompts for sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/SmartScreen settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PreventSmartScreenPromptOverride
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: PreventSmartScreenPromptOverride
- Example value:

```
<true/>
```

Back to top

PreventSmartScreenPromptOverrideForFiles

Prevent bypassing of Microsoft Defender SmartScreen warnings about downloads

Supported versions:

- On Windows since 77 or later
- On macOS since 79 or later

Description

This policy lets you determine whether users can override Microsoft Defender SmartScreen warnings about unverified downloads.

If you enable this policy, users in your organization can't ignore Microsoft Defender SmartScreen warnings, and they're prevented from completing the unverified downloads.

If you disable or don't configure this policy, users can ignore Microsoft Defender SmartScreen warnings and complete unverified downloads.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management, or macOS instances that are that are managed via MDM or joined to a domain via MCX.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PreventSmartScreenPromptOverrideForFiles
- GP name: Prevent bypassing of Microsoft Defender SmartScreen warnings about downloads
- GP path (Mandatory): Administrative Templates/Microsoft Edge/SmartScreen settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PreventSmartScreenPromptOverrideForFiles
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: PreventSmartScreenPromptOverrideForFiles
- Example value:

```
<true/>
```

Back to top

SmartScreenAllowListDomains

Configure the list of domains for which Microsoft Defender SmartScreen won't trigger warnings

Supported versions:

- On Windows and macOS since 77 or later

Description

Configure the list of Microsoft Defender SmartScreen trusted domains. This means: Microsoft Defender SmartScreen won't check for potentially malicious resources like phishing software and other malware if the

source URLs match these domains. The Microsoft Defender SmartScreen download protection service won't check downloads hosted on these domains.

If you enable this policy, Microsoft Defender SmartScreen trusts these domains. If you disable or don't set this policy, default Microsoft Defender SmartScreen protection is applied to all resources.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management, or macOS instances that are that are managed via MDM or joined to a domain via MCX. Also note that this policy does not apply if your organization has enabled Microsoft Defender Advanced Threat Protection. You must configure your allow and block lists in Microsoft Defender Security Center instead.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SmartScreenAllowListDomains
- GP name: Configure the list of domains for which Microsoft Defender SmartScreen won't trigger warnings
- GP path (Mandatory): Administrative Templates/Microsoft Edge/SmartScreen settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\SmartScreenAllowListDomains
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\SmartScreenAllowListDomains\1 = "mydomain.com"
SOFTWARE\Policies\Microsoft\Edge\SmartScreenAllowListDomains\2 = "myuniversity.edu"
```

Mac information and settings

- Preference Key Name: SmartScreenAllowListDomains
- Example value:

```
<array>
  <string>mydomain.com</string>
  <string>myuniversity.edu</string>
</array>
```

Back to top

SmartScreenDnsRequestsEnabled

Enable Microsoft Defender SmartScreen DNS requests

Supported versions:

- On Windows and macOS since 97 or later

Description

This policy lets you configure whether to enable DNS requests made by Microsoft Defender SmartScreen. Note: Disabling DNS requests will prevent Microsoft Defender SmartScreen from getting IP addresses, and potentially impact the IP-based protections provided.

If you enable or don't configure this setting, Microsoft Defender SmartScreen will make DNS requests.

If you disable this setting, Microsoft Defender SmartScreen will not make any DNS requests.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management, or macOS instances that are that are managed via MDM or joined to a domain via MCX.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SmartScreenDnsRequestsEnabled
- GP name: Enable Microsoft Defender SmartScreen DNS requests
- GP path (Mandatory): Administrative Templates/Microsoft Edge/SmartScreen settings
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/SmartScreen settings
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: SmartScreenDnsRequestsEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: SmartScreenDnsRequestsEnabled
- Example value:

```
<true/>
```

Back to top

SmartScreenEnabled

Configure Microsoft Defender SmartScreen

Supported versions:

- On Windows and macOS since 77 or later

Description

This policy setting lets you configure whether to turn on Microsoft Defender SmartScreen. Microsoft Defender SmartScreen provides warning messages to help protect your users from potential phishing scams and malicious software. By default, Microsoft Defender SmartScreen is turned on.

If you enable this setting, Microsoft Defender SmartScreen is turned on.

If you disable this setting, Microsoft Defender SmartScreen is turned off.

If you don't configure this setting, users can choose whether to use Microsoft Defender SmartScreen.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management, or macOS instances that are that are managed via MDM or joined to a domain via MCX.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SmartScreenEnabled
- GP name: Configure Microsoft Defender SmartScreen
- GP path (Mandatory): Administrative Templates/Microsoft Edge/SmartScreen settings
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/SmartScreen settings
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: SmartScreenEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: SmartScreenEnabled
- Example value:

```
<true/>
```

Back to top

SmartScreenForTrustedDownloadsEnabled

Force Microsoft Defender SmartScreen checks on downloads from trusted sources

Supported versions:

- On Windows since 78 or later

Description

This policy setting lets you configure whether Microsoft Defender SmartScreen checks download reputation from a trusted source.

In Windows, the policy determines a trusted source by checking its Internet zone. If the source comes from the local system, intranet, or trusted sites zone, then the download is considered trusted and safe.

If you enable or don't configure this setting, Microsoft Defender SmartScreen checks the download's reputation regardless of source.

If you disable this setting, Microsoft Defender SmartScreen doesn't check the download's reputation when downloading from a trusted source.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SmartScreenForTrustedDownloadsEnabled
- GP name: Force Microsoft Defender SmartScreen checks on downloads from trusted sources
- GP path (Mandatory): Administrative Templates/Microsoft Edge/SmartScreen settings
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/SmartScreen settings
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: SmartScreenForTrustedDownloadsEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

SmartScreenPuaEnabled

Configure Microsoft Defender SmartScreen to block potentially unwanted apps

Supported versions:

- On Windows and macOS since 80 or later

Description

This policy setting lets you configure whether to turn on blocking for potentially unwanted apps with Microsoft Defender SmartScreen. Potentially unwanted app blocking with Microsoft Defender SmartScreen provides warning messages to help protect users from adware, coin miners, bundleware, and other low-reputation apps that are hosted by websites. Potentially unwanted app blocking with Microsoft Defender SmartScreen is turned off by default.

If you enable this setting, potentially unwanted app blocking with Microsoft Defender SmartScreen is turned on.

If you disable this setting, potentially unwanted app blocking with Microsoft Defender SmartScreen is turned off.

If you don't configure this setting, users can choose whether to use potentially unwanted app blocking with Microsoft Defender SmartScreen.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain,

Windows 10 Pro or Enterprise instances that enrolled for device management, or macOS instances that are that are managed via MDM or joined to a domain via MCX.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SmartScreenPuaEnabled
- GP name: Configure Microsoft Defender SmartScreen to block potentially unwanted apps
- GP path (Mandatory): Administrative Templates/Microsoft Edge/SmartScreen settings
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/SmartScreen settings
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: SmartScreenPuaEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: SmartScreenPuaEnabled
- Example value:

```
<true/>
```

Back to top

Startup, home page and new tab page policies

Back to top

HomepageIsNewTabPage

Set the new tab page as the home page

Supported versions:

- On Windows and macOS since 77 or later

Description

Configures the default home page in Microsoft Edge. You can set the home page to a URL you specify or to the new tab page.

If you enable this policy, the Home button is set to the new tab page as configured by the user or with the policy NewTabPageLocation and the URL set with the policy HomepageLocation is not taken into consideration.

If you disable this policy, the Home button is the set URL as configured by the user or as configured in the policy

HomepageLocation.

If you don't configure this policy, users can choose whether the set URL or the new tab page is their home page.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain or Windows 10 Pro or Enterprise instances enrolled for device management.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: HomepageIsNewTabPage
- GP name: Set the new tab page as the home page
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Startup, home page and new tab page
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Startup, home page and new tab page
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: HomepageIsNewTabPage
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: HomepageIsNewTabPage
- Example value:

```
<true/>
```

Back to top

HomepageLocation

Configure the home page URL

Supported versions:

- On Windows and macOS since 77 or later

Description

Configures the default home page URL in Microsoft Edge.

The home page is the page opened by the Home button. The pages that open on startup are controlled by the RestoreOnStartup policies.

You can either set a URL here or set the home page to open the new tab page 'edge://newtab'. By default, the Home button will open the new tab page (as configured by the user or with the policy NewTabPageLocation), and the user will be able to choose between the URL configured by this policy and the new tab page.

If you enable this policy, users can't change their home page URL, but they can choose the behavior for the Home button to open either the set URL or the new tab page. If you wish to enforce the usage of the set URL you must also configure HomepageIsNewTabPage=Disabled.

If you disable or don't configure this policy, users can choose their own home page, as long as the HomepageIsNewTabPage policy isn't enabled.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro, or Enterprise instances enrolled for device management.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: HomepageLocation
- GP name: Configure the home page URL
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Startup, home page and new tab page
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Startup, home page and new tab page
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: HomepageLocation
- Value Type: REG_SZ

Example value:

```
"https://www.contoso.com"
```

Mac information and settings

- Preference Key Name: HomepageLocation
- Example value:

```
<string>https://www.contoso.com</string>
```

Back to top

NewTabPageAllowedBackgroundTypes

Configure the background types allowed for the new tab page layout

Supported versions:

- On Windows and macOS since 86 or later

Description

You can configure which types of background image that are allowed on the new tab page layout in Microsoft Edge.

If you don't configure this policy, all background image types on the new tab page are enabled.

Policy options mapping:

- DisableImageOfTheDay (1) = Disable daily background image type
- DisableCustomImage (2) = Disable custom background image type
- DisableAll (3) = Disable all background image types

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NewTabPageAllowedBackgroundTypes
- GP name: Configure the background types allowed for the new tab page layout
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Startup, home page and new tab page
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: NewTabPageAllowedBackgroundTypes
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: NewTabPageAllowedBackgroundTypes
- Example value:

```
<integer>2</integer>
```

Back to top

NewTabPageAppLauncherEnabled

Hide App Launcher on Microsoft Edge new tab page

Supported versions:

- On Windows and macOS since 108 or later

Description

By default, the App Launcher is shown every time a user opens a new tab page.

If you enable or don't configure this policy, there is no change on the Microsoft Edge new tab page and App Launcher is there for users.

If you disable this policy, App Launcher doesn't appear and users won't be able to launch M365 apps from Microsoft Edge new tab page via the App Launcher.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NewTabPageAppLauncherEnabled
- GP name: Hide App Launcher on Microsoft Edge new tab page
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Startup, home page and new tab page
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: NewTabPageAppLauncherEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: NewTabPageAppLauncherEnabled
- Example value:

```
<false/>
```

Back to top

NewTabPageCompanyLogo

Set new tab page company logo (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 85.

Supported versions:

- On Windows and macOS since 79, until 85

Description

This policy didn't work as expected due to changes in operational requirements. Therefore it's obsolete and should not be used.

Specifies the company logo to use on the new tab page in Microsoft Edge.

The policy should be configured as a string that expresses the logo(s) in JSON format. For example: { "default_logo": { "url": "https://www.contoso.com/logo.png", "hash": "cd0aa9856147b6c5b4ff2b7dfee5da20aa38253099ef1b4a64aced233c9afe29" }, "light_logo": { "url": "https://www.contoso.com/light_logo.png", "hash": "517d286edb416bb2625ccfcba9de78296e90da8e32330d4c9c8275c4c1c33737" } }

You configure this policy by specifying the URL from which Microsoft Edge can download the logo and its cryptographic hash (SHA-256), which is used to verify the integrity of the download. The logo must be in PNG

or SVG format, and its file size must not exceed 16 MB. The logo is downloaded and cached, and it will be redownloaded whenever the URL or the hash changes. The URL must be accessible without any authentication.

The 'default_logo' is required and will be used when there's no background image. If 'light_logo' is provided, it will be used when the user's new tab page has a background image. We recommend a horizontal logo with a transparent background that is left-aligned and vertically centered. The logo should have a minimum height of 32 pixels and an aspect ratio from 1:1 to 4:1. The 'default_logo' should have proper contrast against a white/black background while the 'light_logo' should have proper contrast against a background image.

If you enable this policy, Microsoft Edge downloads and shows the specified logo(s) on the new tab page. Users can't override or hide the logo(s).

If you disable or don't configure this policy, Microsoft Edge will show no company logo or a Microsoft logo on the new tab page.

For help with determining the SHA-256 hash, see Get-FileHash.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Dictionary

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NewTabPageCompanyLogo
- GP name: Set new tab page company logo (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Startup, home page and new tab page
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: NewTabPageCompanyLogo
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\NewTabPageCompanyLogo = {
  "default_logo": {
    "hash": "cd0aa9856147b6c5b4ff2b7dfee5da20aa38253099ef1b4a64aced233c9afe29",
    "url": "https://www.contoso.com/logo.png"
  },
  "light_logo": {
    "hash": "517d286edb416bb2625ccfcba9de78296e90da8e32330d4c9c8275c4c1c33737",
    "url": "https://www.contoso.com/light_logo.png"
  }
}
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\NewTabPageCompanyLogo = {"default_logo": {"hash":
"cd0aa9856147b6c5b4ff2b7dfee5da20aa38253099ef1b4a64aced233c9afe29", "url":
"https://www.contoso.com/logo.png"}, "light_logo": {"hash":
"517d286edb416bb2625ccfcba9de78296e90da8e32330d4c9c8275c4c1c33737", "url":
"https://www.contoso.com/light_logo.png"}}
```

Mac information and settings

- Preference Key Name: NewTabPageCompanyLogo
- Example value:

```
<key>NewTabPageCompanyLogo</key>
<dict>
  <key>default_logo</key>
  <dict>
    <key>hash</key>
    <string>cd0aa9856147b6c5b4ff2b7dfee5da20aa38253099ef1b4a64aced233c9afe29</string>
    <key>url</key>
    <string>https://www.contoso.com/logo.png</string>
  </dict>
  <key>light_logo</key>
  <dict>
    <key>hash</key>
    <string>517d286edb416bb2625ccfcba9de78296e90da8e32330d4c9c8275c4c1c33737</string>
    <key>url</key>
    <string>https://www.contoso.com/light_logo.png</string>
  </dict>
</dict>
```

Back to top

NewTabPageContentEnabled

Allow Microsoft News content on the new tab page

Supported versions:

- On Windows and macOS since 91 or later

Description

If you enable or don't configure this policy, Microsoft Edge displays Microsoft News content on the new tab page. The user can choose different display options for the content, including but not limited to Content off, Content visible on scroll, Headings only, and Content visible. Enabling this policy doesn't force content to be visible - the user can continue to set their own preferred content position.

If you disable this policy, Microsoft Edge does not display Microsoft News content on the new tab page, the Content control in the NTP settings flyout is disabled and set to 'Content off'.

This policy only applies for Microsoft Edge local user profiles, profiles signed in using a Microsoft Account, and profiles signed in using Active Directory. To configure the Enterprise new tab page for profiles signed in using Azure Active Directory, use the M365 admin portal.

Related policies: NewTabPageAllowedBackgroundTypes, NewTabPageQuickLinksEnabled

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NewTabPageContentEnabled
- GP name: Allow Microsoft News content on the new tab page
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Startup, home page and new tab page
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: NewTabPageContentEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: NewTabPageContentEnabled
- Example value:

```
<false/>
```

Back to top

NewTabPageHideDefaultTopSites

Hide the default top sites from the new tab page

Supported versions:

- On Windows and macOS since 77 or later

Description

Hides the default top sites from the new tab page in Microsoft Edge.

If you set this policy to true, the default top site tiles are hidden.

If you set this policy to false or don't configure it, the default top site tiles remain visible.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NewTabPageHideDefaultTopSites
- GP name: Hide the default top sites from the new tab page
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Startup, home page and new tab page
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A

- Value Name: NewTabPageHideDefaultTopSites
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: NewTabPageHideDefaultTopSites
- Example value:

```
<true/>
```

Back to top

NewTabPageLocation

Configure the new tab page URL

Supported versions:

- On Windows and macOS since 77 or later

Description

Configures the default URL for the new tab page.

The recommended version of this policy does not currently work and functions exactly like the mandatory version.

This policy determines the page that's opened when new tabs are created (including when new windows are opened). It also affects the startup page if that's set to open to the new tab page.

This policy doesn't determine which page opens on startup; that's controlled by the RestoreOnStartup policy. It also doesn't affect the home page if that's set to open to the new tab page.

If you don't configure this policy, the default new tab page is used.

If you configure this policy *and* the NewTabPageSetFeedType policy, this policy has precedence.

If a blank tab is preferred, "about:blank" is the correct URL to use, not "about://blank".

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management, or macOS instances that are that are managed via MDM or joined to a domain via MCX.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NewTabPageLocation
- GP name: Configure the new tab page URL
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Startup, home page and new tab page
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Startup, home page and new tab page

- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: NewTabPageLocation
- Value Type: REG_SZ

Example value:

```
"https://www.fabrikam.com"
```

Mac information and settings

- Preference Key Name: NewTabPageLocation
- Example value:

```
<string>https://www.fabrikam.com</string>
```

Back to top

NewTabPageManagedQuickLinks

Set new tab page quick links

Supported versions:

- On Windows and macOS since 79 or later

Description

By default, Microsoft Edge displays quick links on the new tab page from user-added shortcuts and top sites based on browsing history. With this policy, you can configure up to three quick link tiles on the new tab page, expressed as a JSON object:

[{ "url": "https://www.contoso.com", "title": "Contoso Portal", "pinned": true/false }, ...]

The 'url' field is required; 'title' and 'pinned' are optional. If 'title' is not provided, the URL is used as the default title. If 'pinned' is not provided, the default value is false.

Microsoft Edge presents these in the order listed, from left to right, with all pinned tiles displayed ahead of non-pinned tiles.

If the policy is set as mandatory, the 'pinned' field will be ignored and all tiles will be pinned. The tiles can't be deleted by the user and will always appear at the front of the quick links list.

If the policy is set as recommended, pinned tiles will remain in the list but the user has the ability to edit and delete them. Quick link tiles that aren't pinned behave like default top sites and are pushed off the list if other websites are visited more frequently. When applying non-pinned links via this policy to an existing browser profile, the links may not appear at all, depending on how they rank compared to the user's browsing history.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Dictionary

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NewTabPageManagedQuickLinks

- GP name: Set new tab page quick links
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Startup, home page and new tab page
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Startup, home page and new tab page
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: NewTabPageManagedQuickLinks
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\NewTabPageManagedQuickLinks = [
  {
    "pinned": true,
    "title": "Contoso Portal",
    "url": "https://contoso.com"
  },
  {
    "title": "Fabrikam",
    "url": "https://fabrikam.com"
  }
]
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\NewTabPageManagedQuickLinks = [{"pinned": true, "title": "Contoso Portal",
"url": "https://contoso.com"}, {"title": "Fabrikam", "url": "https://fabrikam.com"}]
```

Mac information and settings

- Preference Key Name: NewTabPageManagedQuickLinks
- Example value:

```
<key>NewTabPageManagedQuickLinks</key>
<array>
  <dict>
    <key>pinned</key>
    <true/>
    <key>title</key>
    <string>Contoso Portal</string>
    <key>url</key>
    <string>https://contoso.com</string>
  </dict>
  <dict>
    <key>title</key>
    <string>Fabrikam</string>
    <key>url</key>
    <string>https://fabrikam.com</string>
  </dict>
</array>
```

Back to top

NewTabPagePrerenderEnabled

Enable preload of the new tab page for faster rendering

Supported versions:

- On Windows and macOS since 85 or later

Description

If you configure this policy, preloading the New tab page is enabled, and users can't change this setting. If you don't configure this policy, preloading is enabled and a user can change this setting.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NewTabPagePrerenderEnabled
- GP name: Enable preload of the new tab page for faster rendering
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Startup, home page and new tab page
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Startup, home page and new tab page
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: NewTabPagePrerenderEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: NewTabPagePrerenderEnabled
- Example value:

```
<true/>
```

Back to top

NewTabPageQuickLinksEnabled

Allow quick links on the new tab page

Supported versions:

- On Windows and macOS since 91 or later

Description

If you enable or don't configure this policy, Microsoft Edge displays quick links on the new tab page, and the user can interact with the control, turning quick links on and off. Enabling this policy does not force quick links to be visible - the user can continue to turn quick links on and off.

If you disable this policy, Microsoft Edge hides quick links on the new tab page and disables the quick links control in the NTP settings flyout.

This policy only applies for Microsoft Edge local user profiles, profiles signed in using a Microsoft Account, and profiles signed in using Active Directory. To configure the Enterprise new tab page for profiles signed in using Azure Active Directory, use the M365 admin portal.

Related policies: NewTabPageAllowedBackgroundTypes, NewTabPageContentEnabled

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NewTabPageQuickLinksEnabled
- GP name: Allow quick links on the new tab page
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Startup, home page and new tab page
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: NewTabPageQuickLinksEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: NewTabPageQuickLinksEnabled
- Example value:

```
<true/>
```

Back to top

NewTabPageSetFeedType

Configure the Microsoft Edge new tab page experience (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 92.

Supported versions:

- On Windows and macOS since 79, until 92

Description

This policy is obsolete because the new version of the enterprise new tab page no longer requires choosing between different content types. Instead, the content that is presented to the user can be controlled via the Microsoft 365 admin center. To get to the Microsoft 365 admin center, sign in at https://admin.microsoft.com with your admin account.

Lets you choose either the Microsoft News or Office 365 feed experience for the new tab page.

When you set this policy to 'News', users will see the Microsoft News feed experience on the new tab page.

When you set this policy to 'Office', users with an Azure Active Directory browser sign-in will see the Office 365 feed experience on the new tab page.

If you disable or don't configure this policy:

- Users with an Azure Active Directory browser sign-in are offered the Office 365 new tab page feed experience, as well as the standard new tab page feed experience.
- Users without an Azure Active Directory browser sign-in will see the standard new tab page experience.

If you configure this policy *and* the NewTabPageLocation policy, NewTabPageLocation has precedence.

Default setting: Disabled or not configured.

Policy options mapping:

- News (0) = Microsoft News feed experience
- Office (1) = Office 365 feed experience

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NewTabPageSetFeedType
- GP name: Configure the Microsoft Edge new tab page experience (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Startup, home page and new tab page
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Startup, home page and new tab page
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: NewTabPageSetFeedType
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: NewTabPageSetFeedType
- Example value:

```
<integer>0</integer>
```

Back to top

RestoreOnStartup

Action to take on startup

Supported versions:

- On Windows and macOS since 77 or later

Description

Specify how Microsoft Edge behaves when it starts.

If you want a new tab to always open on startup, choose 'RestoreOnStartupIsNewTabPage'.

If you want to reopen URLs that were open the last time Microsoft Edge closed, choose 'RestoreOnStartupIsLastSession'. The browsing session will be restored as it was. Note that this option disables some settings that rely on sessions or that perform actions on exit (such as Clear browsing data on exit or session-only cookies).

If you want to open a specific set of URLs, choose 'RestoreOnStartupIsURLs'.

Disabling this setting is equivalent to leaving it not configured. Users will be able to change it in Microsoft Edge.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management, or macOS instances that are that are managed via MDM or joined to a domain via MCX.

Policy options mapping:

- RestoreOnStartupIsNewTabPage (5) = Open a new tab
- RestoreOnStartupIsLastSession (1) = Restore the last session
- RestoreOnStartupIsURLs (4) = Open a list of URLs

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: RestoreOnStartup
- GP name: Action to take on startup
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Startup, home page and new tab page
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Startup, home page and new tab page
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: RestoreOnStartup
- Value Type: REG_DWORD

Example value:

```
0x00000004
```

Mac information and settings

- Preference Key Name: RestoreOnStartup

- Example value:

```
<integer>4</integer>
```

Back to top

RestoreOnStartupURLs

Sites to open when the browser starts

Supported versions:

- On Windows and macOS since 77 or later

Description

Specify a list of websites to open automatically when the browser starts. If you don't configure this policy, no site is opened on startup.

This policy only works if you also set the RestoreOnStartup policy to 'Open a list of URLs' (4).

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management, or macOS instances that are that are managed via MDM or joined to a domain via MCX.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: RestoreOnStartupURLs
- GP name: Sites to open when the browser starts
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Startup, home page and new tab page
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Startup, home page and new tab page
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\RestoreOnStartupURLs
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended\RestoreOnStartupURLs
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\RestoreOnStartupURLs\1 = "https://contoso.com"
SOFTWARE\Policies\Microsoft\Edge\RestoreOnStartupURLs\2 = "https://www.fabrikam.com"
```

Mac information and settings

- Preference Key Name: RestoreOnStartupURLs
- Example value:

```
<array>
  <string>https://contoso.com</string>
  <string>https://www.fabrikam.com</string>
</array>
```

Back to top

RestoreOnStartupUserURLsEnabled

Allow users to add and remove their own sites during startup when the RestoreOnStartupURLs policy is configured

Supported versions:

- On Windows and macOS since 107 or later

Description

If you enable this policy, users are allowed to add and remove their own URLs to open when starting Edge while maintaining the admin specified mandatory list of sites specified by setting RestoreOnStartup policy to open a list of URLS and providing the list of sites in the RestoreOnStartupURLs policy.

If you disable or don't configure this policy, there is no change to how the RestoreOnStartup and RestoreOnStartupURLs policies work.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: RestoreOnStartupUserURLsEnabled
- GP name: Allow users to add and remove their own sites during startup when the RestoreOnStartupURLs policy is configured
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Startup, home page and new tab page
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: RestoreOnStartupUserURLsEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: RestoreOnStartupUserURLsEnabled
- Example value:

```
<false/>
```

Back to top

ShowHomeButton

Show Home button on toolbar

Supported versions:

- On Windows and macOS since 77 or later

Description

Shows the Home button on Microsoft Edge's toolbar.

Enable this policy to always show the Home button. Disable it to never show the button.

If you don't configure the policy, users can choose whether to show the home button.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ShowHomeButton
- GP name: Show Home button on toolbar
- GP path (Mandatory): Administrative Templates/Microsoft Edge/Startup, home page and new tab page
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/Startup, home page and new tab page
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ShowHomeButton
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ShowHomeButton
- Example value:

```
<true/>
```

Back to top

TyposquattingChecker settings policies

Back to top

TyposquattingCheckerEnabled

Configure Edge TyposquattingChecker

Supported versions:

- On Windows and macOS since 96 or later

Description

This policy setting lets you configure whether to turn on Edge TyposquattingChecker. Edge TyposquattingChecker provides warning messages to help protect your users from potential typosquatting sites. By default, Edge TyposquattingChecker is turned on.

If you enable this policy, Edge TyposquattingChecker is turned on.

If you disable this policy, Edge TyposquattingChecker is turned off.

If you don't configure this policy, Edge TyposquattingChecker is turned on but users can choose whether to use Edge TyposquattingChecker.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: TyposquattingCheckerEnabled
- GP name: Configure Edge TyposquattingChecker
- GP path (Mandatory): Administrative Templates/Microsoft Edge/TyposquattingChecker settings
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/TyposquattingChecker settings
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: TyposquattingCheckerEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: TyposquattingCheckerEnabled
- Example value:

```
<true/>
```

Back to top

Additional policies

Back to top

AADWebSiteSSOUsingThisProfileEnabled

Single sign-on for work or school sites using this profile enabled

Supported versions:

- On Windows and macOS since 92 or later

Description

'Allow single sign-on for work or school sites using this profile' option allows non-AAD profiles to be able to use single sign-on for work or school sites using work or school credentials present on the machine. This option shows up for end-users as a toggle in Settings -> Profiles -> Profile Preferences for non-AAD profiles only.

If you enable or disable this policy, 'Intelligent enablement of Single sign-on (SSO) for all Windows Azure Active Directory (Azure AD) accounts for users with a single non-Azure AD Microsoft Edge profile' will be turned off.

If you don't configure this policy, users can control whether to use SSO using other credentials present on the machine in edge://settings/profiles/multiProfileSettings.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AADWebSiteSSOUsingThisProfileEnabled
- GP name: Single sign-on for work or school sites using this profile enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: AADWebSiteSSOUsingThisProfileEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: AADWebSiteSSOUsingThisProfileEnabled
- Example value:

```
<false/>
```

Back to top

AccessibilityImageLabelsEnabled

Let screen reader users get image descriptions from Microsoft

Supported versions:

- On Windows and macOS since 97 or later

Description

Lets screen reader users get descriptions of unlabeled images on the web.

If you enable or don't configure this policy, users have the option of using an anonymous Microsoft service. This service provides automatic descriptions for unlabeled images users encounter on the web when they're using a screen reader.

If you disable this policy, users can't enable the Get Image Descriptions from Microsoft feature.

When this feature is enabled, the content of images that need a generated description is sent to Microsoft servers to generate a description.

No cookies or other user data is sent to Microsoft, and Microsoft doesn't save or log any image content.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AccessibilityImageLabelsEnabled
- GP name: Let screen reader users get image descriptions from Microsoft
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AccessibilityImageLabelsEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: AccessibilityImageLabelsEnabled
- Example value:

```
<false/>
```

Back to top

AddressBarEditingEnabled

Configure address bar editing

Supported versions:

- On Windows and macOS since 98 or later

Description

If you enable or don't configure this policy, users can change the URL in the address bar.

If you disable this policy, it prevents users from changing the URL in the address bar.

Note: This policy doesn't prevent the browser from navigating to any URL. Users can still navigate to any URL by using the search option in the default New Tab Page, or using any link that leads to a web search engine. To ensure that users can only go to sites you expect, consider configuring the following policies in addition to this policy:

- NewTabPageLocation

- HomepageLocation
- HomepageIsNewTabPage
- URLBlocklist and URLAllowlist to scope the pages that browser can navigate to.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AddressBarEditingEnabled
- GP name: Configure address bar editing
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AddressBarEditingEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: AddressBarEditingEnabled
- Example value:

```
<true/>
```

Back to top

AddressBarMicrosoftSearchInBingProviderEnabled

Enable Microsoft Search in Bing suggestions in the address bar

Supported versions:

- On Windows and macOS since 81 or later

Description

Enables the display of relevant Microsoft Search in Bing suggestions in the address bar's suggestion list when the user types a search string in the address bar. If you enable or don't configure this policy, users can see internal results powered by Microsoft Search in Bing in the Microsoft Edge address bar suggestion list. To see the Microsoft Search in Bing results, the user must be signed into Microsoft Edge with their Azure AD account for that organization. If you disable this policy, users can't see internal results in the Microsoft Edge address bar suggestion list. Starting with Microsoft Edge version 89, Microsoft Search in Bing suggestions will be available even if Bing isn't the user's default search provider.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No

- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AddressBarMicrosoftSearchInBingProviderEnabled
- GP name: Enable Microsoft Search in Bing suggestions in the address bar
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AddressBarMicrosoftSearchInBingProviderEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: AddressBarMicrosoftSearchInBingProviderEnabled
- Example value:

```
<true/>
```

Back to top

AdsSettingForIntrusiveAdsSites

Ads setting for sites with intrusive ads

Supported versions:

- On Windows and macOS since 78 or later

Description

Controls whether ads are blocked on sites with intrusive ads.

Policy options mapping:

- AllowAds (1) = Allow ads on all sites
- BlockAds (2) = Block ads on sites with intrusive ads. (Default value)

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AdsSettingForIntrusiveAdsSites
- GP name: Ads setting for sites with intrusive ads
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AdsSettingForIntrusiveAdsSites
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: AdsSettingForIntrusiveAdsSites
- Example value:

```
<integer>1</integer>
```

Back to top

AdsTransparencyEnabled

Configure if the ads transparency feature is enabled

Supported versions:

- On Windows and macOS since 100 or later

Description

Lets you decide whether the ads transparency feature is enabled. This behavior only applies to the "balanced" mode of tracking prevention, and does not impact "basic" or "strict" modes. Your users' tracking prevention level can be configured using the TrackingPrevention policy. AdsTransparencyEnabled will only have an effect if TrackingPrevention is set to TrackingPreventionBalanced or is not configured.

If you enable or don't configure this policy, transparency metadata provided by ads will be available to the user when the feature is active.

When the feature is enabled, Tracking Prevention will enable exceptions for the associated ad providers that have met Microsoft's privacy standards.

If you disable this policy, Tracking Prevention will not adjust its behavior even when transparency metadata is provided by ads.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AdsTransparencyEnabled
- GP name: Configure if the ads transparency feature is enabled

- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AdsTransparencyEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: AdsTransparencyEnabled
- Example value:

```
<true/>
```

Back to top

AllowDeletingBrowserHistory

Enable deleting browser and download history

Supported versions:

- On Windows and macOS since 77 or later

Description

Enables deleting browser history and download history and prevents users from changing this setting.

Note that even with this policy is disabled, the browsing and download history aren't guaranteed to be retained: users can edit or delete the history database files directly, and the browser itself may remove (based on expiration period) or archive any or all history items at any time.

If you enable this policy or don't configure it, users can delete the browsing and download history.

If you disable this policy, users can't delete browsing and download history. Disabling this policy will disable history sync and open tab sync.

If you enable this policy, don't enable the ClearBrowsingDataOnExit policy, because they both deal with deleting data. If you enable both, the ClearBrowsingDataOnExit policy takes precedence and deletes all data when Microsoft Edge closes, regardless of how this policy is configured.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AllowDeletingBrowserHistory
- GP name: Enable deleting browser and download history
- GP path (Mandatory): Administrative Templates/Microsoft Edge/

- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AllowDeletingBrowserHistory
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: AllowDeletingBrowserHistory
- Example value:

```
<true/>
```

Back to top

AllowFileSelectionDialogs

Allow file selection dialogs

Supported versions:

- On Windows and macOS since 77 or later

Description

Allow access to local files by letting Microsoft Edge display file selection dialogs.

If you enable or don't configure this policy, users can open file selection dialogs as normal.

If you disable this policy, whenever the user performs an action that triggers a file selection dialog (like importing favorites, uploading files, or saving links), a message is displayed instead, and the user is assumed to have clicked Cancel on the file selection dialog.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AllowFileSelectionDialogs
- GP name: Allow file selection dialogs
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AllowFileSelectionDialogs
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: AllowFileSelectionDialogs
- Example value:

```
<true/>
```

Back to top

AllowGamesMenu

Allow users to access the games menu

Supported versions:

- On Windows and macOS since 99 or later

Description

If you enable or don't configure this policy, users can access the games menu.

If you disable this policy, users won't be able to access the games menu.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AllowGamesMenu
- GP name: Allow users to access the games menu
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AllowGamesMenu
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: AllowGamesMenu
- Example value:

```
<false/>
```

Back to top

AllowPopupsDuringPageUnload

Allows a page to show popups during its unloading (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 87.

Supported versions:

- On Windows and macOS since 78, until 87

Description

This policy allows an admin to specify that a page can show popups during its unloading.

When the policy is set to enabled, pages are allowed to show popups while they're being unloaded.

When the policy is set to disabled or unset, pages aren't allowed to show popups while they're being unloaded. This is as per the spec: (https://html.spec.whatwg.org/#apis-for-creating-and-navigating-browsing-contexts-by-name).

This policy was removed in Microsoft Edge 88 and is ignored if set.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AllowPopupsDuringPageUnload
- GP name: Allows a page to show popups during its unloading (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AllowPopupsDuringPageUnload
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: AllowPopupsDuringPageUnload
- Example value:

```
<false/>
```

Back to top

AllowSurfGame

Allow surf game

Supported versions:

- On Windows and macOS since 83 or later

Description

If you disable this policy, users won't be able to play the surf game when the device is offline or if the user navigates to edge://surf.

If you enable or don't configure this policy, users can play the surf game.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AllowSurfGame
- GP name: Allow surf game
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AllowSurfGame
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: AllowSurfGame
- Example value:

```
<false/>
```

Back to top

AllowSyncXHRInPageDismissal

Allow pages to send synchronous XHR requests during page dismissal (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 99.

Supported versions:

- On Windows and macOS since 79, until 99

Description

This policy is obsolete because it was only intended to be a short-term mechanism to give enterprises more time to update their web content if and when it was found to be incompatible with the change to disallow synchronous XHR requests during page dismissal. It doesn't work in Microsoft Edge after version 99.

This policy lets you specify that a page can send synchronous XHR requests during page dismissal.

If you enable this policy, pages can send synchronous XHR requests during page dismissal.

If you disable this policy or don't configure this policy, pages aren't allowed to send synchronous XHR requests during page dismissal.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AllowSyncXHRInPageDismissal
- GP name: Allow pages to send synchronous XHR requests during page dismissal (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AllowSyncXHRInPageDismissal
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: AllowSyncXHRInPageDismissal
- Example value:

```
<false/>
```

Back to top

AllowTokenBindingForUrls

Configure the list of sites for which Microsoft Edge will attempt to establish a Token Binding with

Supported versions:

- On Windows since 83 or later

Description

Configure the list of URL patterns for sites that the browser will attempt to perform the Token Binding protocol with. For the domains on this list, the browser will send the Token Binding ClientHello in the TLS handshake (See https://tools.ietf.org/html/rfc8472). If the server responds with a valid ServerHello response, the browser will create and send Token Binding messages on subsequent https requests. See https://tools.ietf.org/html/rfc8471 for more info.

If this list is empty, Token Binding will be disabled.

This policy is only available on Windows 10 devices with Virtual Secure Mode capability.

Starting in Microsoft Edge 86, this policy no longer supports dynamic refresh.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AllowTokenBindingForUrls
- GP name: Configure the list of sites for which Microsoft Edge will attempt to establish a Token Binding with
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\AllowTokenBindingForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\AllowTokenBindingForUrls\1 = "mydomain.com"
SOFTWARE\Policies\Microsoft\Edge\AllowTokenBindingForUrls\2 = "[*.]mydomain2.com"
SOFTWARE\Policies\Microsoft\Edge\AllowTokenBindingForUrls\3 = "[*.].mydomain2.com"
```

Back to top

AllowTrackingForUrls

Configure tracking prevention exceptions for specific sites

Supported versions:

- On Windows and macOS since 78 or later

Description

Configure the list of URL patterns that are excluded from tracking prevention.

If you configure this policy, the list of configured URL patterns is excluded from tracking prevention.

If you don't configure this policy, the global default value from the "Block tracking of users' web-browsing activity" policy (if set) or the user's personal configuration is used for all sites.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AllowTrackingForUrls
- GP name: Configure tracking prevention exceptions for specific sites

- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\AllowTrackingForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\AllowTrackingForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\AllowTrackingForUrls\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: AllowTrackingForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

AllowedDomainsForApps

Define domains allowed to access Google Workspace

Supported versions:

- On Windows and macOS since 104 or later

Description

Setting the policy on Microsoft Edge turns on the restricted sign-in feature in Google Workspace and prevents users from changing this setting. Users can only access Google tools using accounts from the specified domains. To allow gmail or googlemail accounts, add consumer_accounts to the list of domains. This policy is based on the Chrome policy of the same name.

If you don't provide a domain name or leave this policy unset, users can access Google Workspace with any account.

Users cannot change or override this setting.

Note: This policy causes the X-GoogApps-Allowed-Domains header to be appended to all HTTP and HTTPS requests to all google.com domains, as described in https://go.microsoft.com/fwlink/?linkid=2197973.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AllowedDomainsForApps

- GP name: Define domains allowed to access Google Workspace
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AllowedDomainsForApps
- Value Type: REG_SZ

Example value:

```
"example.com"
```

Mac information and settings

- Preference Key Name: AllowedDomainsForApps
- Example value:

```
<string>example.com</string>
```

Back to top

AlternateErrorPagesEnabled

Suggest similar pages when a webpage can't be found

Supported versions:

- On Windows and macOS since 80 or later

Description

Allow Microsoft Edge to issue a connection to a web service to generate URL and search suggestions for connectivity issues such as DNS errors.

If you enable this policy, a web service is used to generate url and search suggestions for network errors.

If you disable this policy, no calls to the web service are made and a standard error page is shown.

If you don't configure this policy, Microsoft Edge respects the user preference that's set under Services at edge://settings/privacy. Specifically, there's a **Suggest similar pages when a webpage can't be found** toggle, which the user can switch on or off. Note that if you have enable this policy (AlternateErrorPagesEnabled), the Suggest similar pages when a webpage can't be found setting is turned on, but the user can't change the setting by using the toggle. If you disable this policy, the Suggest similar pages when a webpage can't be found setting is turned off, and the user can't change the setting by using the toggle.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AlternateErrorPagesEnabled
- GP name: Suggest similar pages when a webpage can't be found
- GP path (Mandatory): Administrative Templates/Microsoft Edge/

- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: AlternateErrorPagesEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: AlternateErrorPagesEnabled
- Example value:

```
<true/>
```

Back to top

AlwaysOpenPdfExternally

Always open PDF files externally

Supported versions:

- On Windows and macOS since 77 or later

Description

Disables the internal PDF viewer in Microsoft Edge.

If you enable this policy Microsoft Edge treats PDF files as downloads and lets users open them with the default application.

If Microsoft Edge is the default PDF reader, PDF files aren't downloaded and will continue to open in Microsoft Edge.

If you don't configure this policy or disable it, Microsoft Edge will open PDF files (unless the user disables it).

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AlwaysOpenPdfExternally
- GP name: Always open PDF files externally
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A

- Value Name: AlwaysOpenPdfExternally
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: AlwaysOpenPdfExternally
- Example value:

```
<true/>
```

Back to top

AmbientAuthenticationInPrivateModesEnabled

Enable Ambient Authentication for InPrivate and Guest profiles

Supported versions:

- On Windows and macOS since 81 or later

Description

Configure this policy to allow/disallow ambient authentication for InPrivate and Guest profiles in Microsoft Edge.

Ambient Authentication is http authentication with default credentials when explicit credentials aren't provided via NTLM/Kerberos/Negotiate challenge/response schemes.

If you set the policy to 'RegularOnly', it allows ambient authentication for Regular sessions only. InPrivate and Guest sessions won't be allowed to ambiently authenticate.

If you set the policy to 'InPrivateAndRegular', it allows ambient authentication for InPrivate and Regular sessions. Guest sessions won't be allowed to ambiently authenticate.

If you set the policy to 'GuestAndRegular', it allows ambient authentication for Guest and Regular sessions. InPrivate sessions won't be allowed to ambiently authenticate

If you set the policy to 'All', it allows ambient authentication for all sessions.

Note that ambient authentication is always allowed on regular profiles.

In Microsoft Edge version 81 and later, if the policy is left not set, ambient authentication will be enabled in regular sessions only.

Policy options mapping:

- RegularOnly (0) = Enable ambient authentication in regular sessions only
- InPrivateAndRegular (1) = Enable ambient authentication in InPrivate and regular sessions
- GuestAndRegular (2) = Enable ambient authentication in guest and regular sessions
- All (3) = Enable ambient authentication in regular, InPrivate and guest sessions

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AmbientAuthenticationInPrivateModesEnabled
- GP name: Enable Ambient Authentication for InPrivate and Guest profiles
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AmbientAuthenticationInPrivateModesEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: AmbientAuthenticationInPrivateModesEnabled
- Example value:

```
<integer>0</integer>
```

Back to top

AppCacheForceEnabled

Allows the AppCache feature to be re-enabled, even if it's turned off by default (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 96.

Supported versions:

- On Windows and macOS since 84, until 96

Description

Support for AppCache and this policy was removed from Microsoft Edge starting in version 97.

If you set this policy to true, the AppCache is enabled, even when AppCache in Microsoft Edge is not available by default.

If you set this policy to false, or don't set it, AppCache will follow Microsoft Edge's defaults.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AppCacheForceEnabled

- GP name: Allows the AppCache feature to be re-enabled, even if it's turned off by default (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AppCacheForceEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: AppCacheForceEnabled
- Example value:

```
<false/>
```

Back to top

ApplicationLocaleValue

Set application locale

Supported versions:

- On Windows since 77 or later

Description

Configures the application locale in Microsoft Edge and prevents users from changing the locale.

If you enable this policy, Microsoft Edge uses the specified locale. If the configured locale isn't supported, 'en-US' is used instead.

If you disable or don't configure this setting, Microsoft Edge uses either the user-specified preferred locale (if configured) or the fallback locale 'en-US'.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ApplicationLocaleValue
- GP name: Set application locale
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended

- Value Name: ApplicationLocaleValue
- Value Type: REG_SZ

Example value:

```
"en"
```

Back to top

AskBeforeCloseEnabled

Get user confirmation before closing a browser window with multiple tabs

Supported versions:

- On Windows and macOS since 104 or later

Description

This policy lets you configure whether users see a confirmation dialog before closing a browser window with multiple tabs. This dialog asks users to confirm that the browser window can be closed.

If you enable this policy, users will be presented with a confirmation dialog when closing a browser window with multiple tabs.

If you disable or don't configure this policy, a browser window with multiple tabs will close immediately without user confirmation.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AskBeforeCloseEnabled
- GP name: Get user confirmation before closing a browser window with multiple tabs
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: AskBeforeCloseEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: AskBeforeCloseEnabled
- Example value:

```
<true/>
```

Back to top

AudioCaptureAllowed

Allow or block audio capture

Supported versions:

- On Windows and macOS since 77 or later

Description

Allows you to set whether a user is prompted to grant a website access to their audio capture device. This policy applies to all URLs except for those configured in the AudioCaptureAllowedUrls list.

If you enable this policy or don't configure it (the default setting), the user is prompted for audio capture access except from the URLs in the AudioCaptureAllowedUrls list. These listed URLs are granted access without prompting.

If you disable this policy, the user is not prompted, and audio capture is accessible only to the URLs configured in AudioCaptureAllowedUrls.

This policy affects all types of audio inputs, not only the built-in microphone.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AudioCaptureAllowed
- GP name: Allow or block audio capture
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AudioCaptureAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: AudioCaptureAllowed
- Example value:

```
<false/>
```

Back to top

AudioCaptureAllowedUrls

Sites that can access audio capture devices without requesting permission

Supported versions:

- On Windows and macOS since 77 or later

Description

Specify websites, based on URL patterns, that can use audio capture devices without asking the user for permission. Patterns in this list are matched against the security origin of the requesting URL. If they match, the site is automatically granted access to audio capture devices.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AudioCaptureAllowedUrls
- GP name: Sites that can access audio capture devices without requesting permission
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\AudioCaptureAllowedUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\AudioCaptureAllowedUrls\1 = "https://www.contoso.com/"
SOFTWARE\Policies\Microsoft\Edge\AudioCaptureAllowedUrls\2 = "https://[*.]contoso.edu/"
```

Mac information and settings

- Preference Key Name: AudioCaptureAllowedUrls
- Example value:

```
<array>
  <string>https://www.contoso.com/</string>
  <string>https://[*.]contoso.edu/</string>
</array>
```

Back to top

AudioProcessHighPriorityEnabled

Allow the audio process to run with priority above normal on Windows

Supported versions:

- On Windows since 96 or later

Description

This policy controls the priority of the audio process on Windows. If this policy is enabled, the audio process will run with above normal priority. If this policy is disabled, the audio process will run with normal priority. If this policy is not configured, the default configuration for the audio process will be used. This policy is intended as a

temporary measure to give enterprises the ability to run audio with higher priority to address certain performance issues with audio capture. This policy will be removed in the future.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AudioProcessHighPriorityEnabled
- GP name: Allow the audio process to run with priority above normal on Windows
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AudioProcessHighPriorityEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

AudioSandboxEnabled

Allow the audio sandbox to run

Supported versions:

- On Windows and macOS since 81 or later

Description

This policy controls the audio process sandbox.

If you enable this policy, the audio process will run sandboxed.

If you disable this policy, the audio process will run unsandboxed and the WebRTC audio-processing module will run in the renderer process. This leaves users open to security risks related to running the audio subsystem unsandboxed.

If you don't configure this policy, the default configuration for the audio sandbox will be used, which might differ based on the platform.

This policy is intended to give enterprises flexibility to disable the audio sandbox if they use security software setups that interfere with the sandbox.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AudioSandboxEnabled
- GP name: Allow the audio sandbox to run
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AudioSandboxEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: AudioSandboxEnabled
- Example value:

```
<true/>
```

Back to top

AutoImportAtFirstRun

Automatically import another browser's data and settings at first run

Supported versions:

- On Windows and macOS since 77 or later

Description

If you enable this policy, all supported datatypes and settings from the specified browser will be silently and automatically imported at first run. During the First Run Experience, the import section will also be skipped.

The browser data from Microsoft Edge Legacy will always be silently migrated at the first run, irrespective of the value of this policy.

If this policy is set to 'FromDefaultBrowser', then the datatypes corresponding to the default browser on the managed device will be imported.

If the browser specified as the value of this policy is not present in the managed device, Microsoft Edge will simply skip the import without any notification to the user.

If you set this policy to 'DisabledAutoImport', the import section of the first-run experience is skipped entirely and Microsoft Edge doesn't import browser data and settings automatically.

If this policy is set to the value of 'FromInternetExplorer', the following datatypes will be imported from Internet Explorer:

1. Favorites or bookmarks
2. Saved passwords
3. Search engines
4. Browsing history
5. Home page

If this policy is set to the value of 'FromGoogleChrome', the following datatypes will be imported from Google Chrome:

1. Favorites
2. Saved passwords
3. Addresses and more
4. Payment info
5. Browsing history
6. Settings
7. Pinned and Open tabs
8. Extensions
9. Cookies

Note: For more details on what is imported from Google Chrome, please see https://go.microsoft.com/fwlink/?linkid=2120835

If this policy is set to the value of 'FromSafari', user data is no longer imported into Microsoft Edge. This is due to the way Full Disk Access works on Mac. On macOS Mojave and above, it's no longer possible to have automated and unattended import of Safari data into Microsoft Edge.

Starting with Microsoft Edge version 83, if this policy is set to the value of 'FromMozillaFirefox', the following datatypes will be imported from Mozilla Firefox:

1. Favorites or bookmarks
2. Saved passwords
3. Addresses and more
4. Browsing History

If you want to restrict specific datatypes from getting imported on the managed devices, you can use this policy with other policies such as ImportAutofillFormData, ImportBrowserSettings, ImportFavorites, and etc.

Policy options mapping:

- FromDefaultBrowser (0) = Automatically imports all supported datatypes and settings from the default browser
- FromInternetExplorer (1) = Automatically imports all supported datatypes and settings from Internet Explorer
- FromGoogleChrome (2) = Automatically imports all supported datatypes and settings from Google Chrome
- FromSafari (3) = Automatically imports all supported datatypes and settings from Safari
- DisabledAutoImport (4) = Disables automatic import, and the import section of the first-run experience is skipped
- FromMozillaFirefox (5) = Automatically imports all supported datatypes and settings from Mozilla Firefox

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AutoImportAtFirstRun
- GP name: Automatically import another browser's data and settings at first run
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AutoImportAtFirstRun
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: AutoImportAtFirstRun
- Example value:

```
<integer>2</integer>
```

Back to top

AutoLaunchProtocolsComponentEnabled

AutoLaunch Protocols Component Enabled

Supported versions:

- On Windows and macOS since 96 or later

Description

Specifies whether the AutoLaunch Protocols component should be enabled. This component allows Microsoft to provide a list similar to that of the AutoLaunchProtocolsFromOrigins policy, allowing certain external protocols to launch without prompt or blocking certain protocols (on specified origins). By default, this component is enabled.

If you enable or don't configure this policy, the AutoLaunch Protocols component is enabled.

If you disable this policy, the AutoLaunch Protocols component is disabled.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AutoLaunchProtocolsComponentEnabled
- GP name: AutoLaunch Protocols Component Enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/

- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AutoLaunchProtocolsComponentEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: AutoLaunchProtocolsComponentEnabled
- Example value:

```
<true/>
```

Back to top

AutoLaunchProtocolsFromOrigins

Define a list of protocols that can launch an external application from listed origins without prompting the user

Supported versions:

- On Windows and macOS since 85 or later

Description

Allows you to set a list of protocols, and for each protocol an associated list of allowed origin patterns, that can launch an external application without prompting the user. The trailing separator should not be included when listing the protocol. For example, list "skype" instead of "skype:" or "skype://".

If you configure this policy, a protocol will only be permitted to launch an external application without prompting by policy if:

- the protocol is listed
- the origin of the site trying to launch the protocol matches one of the origin patterns in that protocol's allowed_origins list.

If either condition is false, the external protocol launch prompt will not be omitted by policy.

If you don't configure this policy, no protocols can launch without a prompt. Users can opt out of prompts on a per-protocol/per-site basis unless the ExternalProtocolDialogShowAlwaysOpenCheckbox policy is set to Disabled. This policy has no impact on per-protocol/per-site prompt exemptions set by users.

The origin matching patterns use a similar format to those for the URLBlocklist policy, which are documented at https://go.microsoft.com/fwlink/?linkid=2095322.

However, origin matching patterns for this policy cannot contain "/path" or "@query" elements. Any pattern that does contain a "/path" or "@query" element will be ignored.

This policy does not work as expected with file://* wildcards.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Dictionary

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AutoLaunchProtocolsFromOrigins
- GP name: Define a list of protocols that can launch an external application from listed origins without prompting the user
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AutoLaunchProtocolsFromOrigins
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\AutoLaunchProtocolsFromOrigins = [
  {
    "allowed_origins": [
      "example.com",
      "http://www.example.com:8080"
    ],
    "protocol": "spotify"
  },
  {
    "allowed_origins": [
      "https://example.com",
      "https://.mail.example.com"
    ],
    "protocol": "msteams"
  },
  {
    "allowed_origins": [
      "*"
    ],
    "protocol": "msoutlook"
  }
]
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\AutoLaunchProtocolsFromOrigins = [{"allowed_origins": ["example.com",
"http://www.example.com:8080"], "protocol": "spotify"}, {"allowed_origins": ["https://example.com",
"https://.mail.example.com"], "protocol": "msteams"}, {"allowed_origins": ["*"], "protocol": "msoutlook"}]
```

Mac information and settings

- Preference Key Name: AutoLaunchProtocolsFromOrigins
- Example value:

```
<key>AutoLaunchProtocolsFromOrigins</key>
<array>
  <dict>
    <key>allowed_origins</key>
    <array>
      <string>example.com</string>
      <string>http://www.example.com:8080</string>
    </array>
    <key>protocol</key>
    <string>spotify</string>
  </dict>
  <dict>
    <key>allowed_origins</key>
    <array>
      <string>https://example.com</string>
      <string>https://.mail.example.com</string>
    </array>
    <key>protocol</key>
    <string>msteams</string>
  </dict>
  <dict>
    <key>allowed_origins</key>
    <array>
      <string>*</string>
    </array>
    <key>protocol</key>
    <string>msoutlook</string>
  </dict>
</array>
```

Back to top

AutoOpenAllowedForURLs

URLs where AutoOpenFileTypes can apply

Supported versions:

- On Windows and macOS since 85 or later

Description

A list of URLs to which AutoOpenFileTypes will apply to. This policy has no impact on automatically open values set by users via the download shelf ... > "Always open files of this type" menu entry.

If you set URLs in this policy, files will only automatically open by policy if the URL is part of this set and the file type is listed in AutoOpenFileTypes. If either condition is false, the download won't automatically open by policy.

If you don't set this policy, all downloads where the file type is in AutoOpenFileTypes will automatically open.

A URL pattern has to be formatted according to https://go.microsoft.com/fwlink/?linkid=2095322.

This policy does not work as expected with file://* wildcards.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AutoOpenAllowedForURLs
- GP name: URLs where AutoOpenFileTypes can apply

- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\AutoOpenAllowedForURLs
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\AutoOpenAllowedForURLs\1 = "example.com"
SOFTWARE\Policies\Microsoft\Edge\AutoOpenAllowedForURLs\2 = "https://ssl.server.com"
SOFTWARE\Policies\Microsoft\Edge\AutoOpenAllowedForURLs\3 = "hosting.com/good_path"
SOFTWARE\Policies\Microsoft\Edge\AutoOpenAllowedForURLs\4 = "https://server:8080/path"
SOFTWARE\Policies\Microsoft\Edge\AutoOpenAllowedForURLs\5 = ".exact.hostname.com"
```

Mac information and settings

- Preference Key Name: AutoOpenAllowedForURLs
- Example value:

```
<array>
  <string>example.com</string>
  <string>https://ssl.server.com</string>
  <string>hosting.com/good_path</string>
  <string>https://server:8080/path</string>
  <string>.exact.hostname.com</string>
</array>
```

Back to top

AutoOpenFileTypes

List of file types that should be automatically opened on download

Supported versions:

- On Windows and macOS since 85 or later

Description

This policy sets a list of file types that should be automatically opened on download. Note: The leading separator should not be included when listing the file type, so list "txt" instead of ".txt".

By default, these file types will be automatically opened on all URLs. You can use the AutoOpenAllowedForURLs policy to restrict the URLs for which these file types will be automatically opened on.

Files with types that should be automatically opened will still be subject to the enabled Microsoft Defender SmartScreen checks and won't be opened if they fail those checks.

File types that a user has already specified to automatically be opened will continue to do so when downloaded. The user will continue to be able to specify other file types to be automatically opened.

If you don't set this policy, only file types that a user has already specified to automatically be opened will do so when downloaded.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management, or macOS instances that are that are managed via MDM or joined to a domain via MCX.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AutoOpenFileTypes
- GP name: List of file types that should be automatically opened on download
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\AutoOpenFileTypes
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\AutoOpenFileTypes\1 = "exe"
SOFTWARE\Policies\Microsoft\Edge\AutoOpenFileTypes\2 = "txt"
```

Mac information and settings

- Preference Key Name: AutoOpenFileTypes
- Example value:

```
<array>
  <string>exe</string>
  <string>txt</string>
</array>
```

Back to top

AutofillAddressEnabled

Enable AutoFill for addresses

Supported versions:

- On Windows and macOS since 77 or later

Description

Enables the AutoFill feature and allows users to auto-complete address information in web forms using previously stored information.

If you disable this policy, AutoFill never suggests or fills in address information, nor does it save additional address information that the user might submit while browsing the web.

If you enable this policy or don't configure it, users can control AutoFill for addresses in the user interface.

Note that if you disable this policy you also stop all activity for all web forms, except payment and password forms. No further entries are saved, and Microsoft Edge won't suggest or AutoFill any previous entries.

Supported features:

- Can be mandatory: Yes

- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AutofillAddressEnabled
- GP name: Enable AutoFill for addresses
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: AutofillAddressEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: AutofillAddressEnabled
- Example value:

```
<false/>
```

Back to top

AutofillCreditCardEnabled

Enable AutoFill for payment instruments

Supported versions:

- On Windows and macOS since 77 or later

Description

Enables Microsoft Edge's AutoFill feature and lets users auto complete payment instruments like credit or debit cards in web forms using previously stored information. This includes suggesting new payment instruments like Buy Now Pay Later (BNPL) in web forms and Express Checkout.

If you enable this policy or don't configure it, users can control AutoFill for payment instruments.

If you disable this policy, AutoFill never suggests, fills, or recommends new payment Instruments. Additionally, it won't save any payment instrument information that users submit while browsing the web.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AutofillCreditCardEnabled
- GP name: Enable AutoFill for payment instruments
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: AutofillCreditCardEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: AutofillCreditCardEnabled
- Example value:

```
<false/>
```

Back to top

AutomaticHttpsDefault

Configure Automatic HTTPS

Supported versions:

- On Windows and macOS since 92 or later

Description

This policy lets you manage settings for AutomaticHttpsDefault, which switches connections from HTTP to HTTPS.

This feature helps protect against man-in-the-middle attacks by enforcing more secure connections, but users might experience more connection errors.

Note: The 'UpgradeCapableDomains' configuration requires a component list, and will not upgrade these connections if ComponentUpdatesEnabled is set to 'Disabled'.

If you don't configure this policy, AutomaticHttpsDefault will be enabled, and will only upgrade connections on domains likely to support HTTPS.

Policy options mapping:

- DisableAutomaticHttps (0) = Automatic HTTPS functionality is disabled.
- UpgradeCapableDomains (1) = Navigations delivered over HTTP are switched to HTTPS, only on domains likely to support HTTPS.
- AlwaysUpgrade (2) = All navigations delivered over HTTP are switched to HTTPS. Connection errors might occur more often.

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes

- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AutomaticHttpsDefault
- GP name: Configure Automatic HTTPS
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: AutomaticHttpsDefault
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: AutomaticHttpsDefault
- Example value:

```
<integer>2</integer>
```

Back to top

AutoplayAllowed

Allow media autoplay for websites

Supported versions:

- On Windows and macOS since 78 or later

Description

This policy sets the media autoplay policy for websites.

The default setting, "Not configured" respects the current media autoplay settings and lets users configure their autoplay settings.

Setting to "Enabled" sets media autoplay to "Allow". All websites are allowed to autoplay media. Users can't override this policy.

Setting to "Disabled" sets media autoplay to "Limit". This limits websites that are allowed to autoplay media to webpages with high media engagement and active WebRTC streams. Prior to Microsoft Edge version 92, this would set media autoplay to "Block". Users can't override this policy.

A tab will need to be closed and re-opened for this policy to take effect.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AutoplayAllowed
- GP name: Allow media autoplay for websites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: AutoplayAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: AutoplayAllowed
- Example value:

```
<true/>
```

Back to top

AutoplayAllowlist

Allow media autoplay on specific sites

Supported versions:

- On Windows and macOS since 93 or later

Description

Define a list of sites, based on URL patterns, that are allowed to autoplay media.

If you don't configure this policy, the global default value from the AutoplayAllowed policy (if set) or the user's personal configuration is used for all sites.

For detailed information about valid url patterns, see https://go.microsoft.com/fwlink/?linkid=2095322.

Note: * is not an accepted value for this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AutoplayAllowlist
- GP name: Allow media autoplay on specific sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/

- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\AutoplayAllowlist
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\AutoplayAllowlist\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\AutoplayAllowlist\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: AutoplayAllowlist
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

BackgroundModeEnabled

Continue running background apps after Microsoft Edge closes

Supported versions:

- On Windows since 77 or later

Description

Allows Microsoft Edge processes to start at OS sign-in and keep running after the last browser window is closed. In this scenario, background apps and the current browsing session remain active, including any session cookies. An open background process displays an icon in the system tray and can always be closed from there.

If you enable this policy, background mode is turned on.

If you disable this policy, background mode is turned off.

If you don't configure this policy, background mode is initially turned off, and the user can configure its behavior in edge://settings/system.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: BackgroundModeEnabled
- GP name: Continue running background apps after Microsoft Edge closes
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/

- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: BackgroundModeEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

BackgroundTemplateListUpdatesEnabled

Enables background updates to the list of available templates for Collections and other features that use templates (deprecated)

> DEPRECATED: This policy is deprecated. It is currently supported but will become obsolete in a future release.

Supported versions:

- On Windows and macOS since 79 or later

Description

This policy is deprecated because we are moving to a new policy. It won't work in Microsoft Edge as soon as version 104. The new policy to use is EdgeAssetDeliveryServiceEnabled.

Lets you enable or disable background updates to the list of available templates for Collections and other features that use templates. Templates are used to extract rich metadata from a webpage when the page is saved to a collection.

If you enable this setting or the setting is unconfigured, the list of available templates will be downloaded in the background from a Microsoft service every 24 hours.

If you disable this setting the list of available templates will be downloaded on demand. This type of download might result in small performance penalties for Collections and other features.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: BackgroundTemplateListUpdatesEnabled
- GP name: Enables background updates to the list of available templates for Collections and other features that use templates (deprecated)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A

- Value Name: BackgroundTemplateListUpdatesEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: BackgroundTemplateListUpdatesEnabled
- Example value:

```
<true/>
```

Back to top

BingAdsSuppression

Block all ads on Bing search results

Supported versions:

- On Windows and macOS since 83 or later

Description

Enables an ad-free search experience on Bing.com

If you enable this policy, then a user can search on bing.com and have an ad-free search experience. At the same time, the SafeSearch setting will be set to 'Strict' and can't be changed by the user.

If you don't configure this policy, then the default experience will have ads in the search results on bing.com. SafeSearch will be set to 'Moderate' by default and can be changed by the user.

This policy is only available for K-12 SKUs that are identified as EDU tenants by Microsoft.

Please refer to https://go.microsoft.com/fwlink/?linkid=2119711 to learn more about this policy or if the following scenarios apply to you:

- You have an EDU tenant, but the policy doesn't work.
- You had your IP allowlisted for having an ad free search experience.
- You were experiencing an ad-free search experience on Microsoft Edge Legacy and want to upgrade to the new version of Microsoft Edge.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: BingAdsSuppression
- GP name: Block all ads on Bing search results
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge

- Path (Recommended): N/A
- Value Name: BingAdsSuppression
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: BingAdsSuppression
- Example value:

```
<true/>
```

Back to top

BlockThirdPartyCookies

Block third party cookies

Supported versions:

- On Windows and macOS since 77 or later

Description

Block web page elements that aren't from the domain that's in the address bar from setting cookies.

If you enable this policy, web page elements that are not from the domain that is in the address bar can't set cookies

If you disable this policy, web page elements from domains other than in the address bar can set cookies.

If you don't configure this policy, third-party cookies are enabled but users can change this setting.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: BlockThirdPartyCookies
- GP name: Block third party cookies
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: BlockThirdPartyCookies
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: BlockThirdPartyCookies
- Example value:

```
<false/>
```

Back to top

BrowserAddProfileEnabled

Enable profile creation from the Identity flyout menu or the Settings page

Supported versions:

- On Windows and macOS since 77 or later

Description

Allows users to create new profiles, using the **Add profile** option. If you enable this policy or don't configure it, Microsoft Edge allows users to use **Add profile** on the Identity flyout menu or the Settings page to create new profiles.

If you disable this policy, users cannot add new profiles from the Identity flyout menu or the Settings page.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: BrowserAddProfileEnabled
- GP name: Enable profile creation from the Identity flyout menu or the Settings page
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: BrowserAddProfileEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: BrowserAddProfileEnabled
- Example value:

```
<true/>
```

Back to top

BrowserCodeIntegritySetting

Configure browser process code integrity guard setting

Supported versions:

- On Windows since 104 or later

Description

This policy controls the use of code integrity guard in the browser process, which only allows Microsoft signed binaries to load.

Setting this policy to Enabled will enable code integrity guard in the browser process.

Setting this policy to Audit or leaving the policy unset will enable audit mode for code integrity guard in the browser process. Audit mode will emit logs to the event viewer under Security-Mitigations and CodeIntegrity providers when a binary is loaded after CIG was enabled that is not Microsoft signed.

Setting this policy to Disabled will prevent the browser from enabling code integrity guard in the browser process.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, or Windows 10 Pro or Enterprise instances that enrolled for device management.

This policy will only take effect on Windows 10 RS2 and above.

Policy options mapping:

- Disabled (0) = Do not enable code integrity guard in the browser process.
- Audit (1) = Enable code integrity guard audit mode in the browser process.
- Enabled (2) = Enable code integrity guard enforcement in the browser process.

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: BrowserCodeIntegritySetting
- GP name: Configure browser process code integrity guard setting
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: BrowserCodeIntegritySetting
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

BrowserGuestModeEnabled

Enable guest mode

Supported versions:

- On Windows and macOS since 77 or later

Description

Enable the option to allow the use of guest profiles in Microsoft Edge. In a guest profile, the browser doesn't import browsing data from existing profiles, and it deletes browsing data when all guest profiles are closed.

If you enable this policy or don't configure it, Microsoft Edge lets users browse in guest profiles.

If you disable this policy, Microsoft Edge doesn't let users browse in guest profiles.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: BrowserGuestModeEnabled
- GP name: Enable guest mode
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: BrowserGuestModeEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: BrowserGuestModeEnabled
- Example value:

```
<true/>
```

Back to top

BrowserLegacyExtensionPointsBlockingEnabled

Enable browser legacy extension point blocking

Supported versions:

- On Windows since 95 or later

Description

Sets the ProcessExtensionPointDisablePolicy on Microsoft Edge's browser process to block code injection from legacy third party applications.

If you enable or don't configure this policy, the ProcessExtensionPointDisablePolicy is applied to block legacy extension points in the browser process.

If you disable this policy, the ProcessExtensionPointDisablePolicy is not applied to block legacy extension points in the browser process. This has a detrimental effect on Microsoft Edge's security and stability as unknown and potentially hostile code can load inside Microsoft Edge's browser process. Only turn off the policy if there are compatibility issues with third-party software that must run inside Microsoft Edge's browser process.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: BrowserLegacyExtensionPointsBlockingEnabled
- GP name: Enable browser legacy extension point blocking
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: BrowserLegacyExtensionPointsBlockingEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

BrowserNetworkTimeQueriesEnabled

Allow queries to a Browser Network Time service

Supported versions:

- On Windows and macOS since 77 or later

Description

Prevents Microsoft Edge from occasionally sending queries to a browser network time service to retrieve an accurate timestamp.

If you disable this policy, Microsoft Edge will stop sending queries to a browser network time service.

If you enable this policy or don't configure it, Microsoft Edge will occasionally send queries to a browser network time service.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: BrowserNetworkTimeQueriesEnabled
- GP name: Allow queries to a Browser Network Time service
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: BrowserNetworkTimeQueriesEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: BrowserNetworkTimeQueriesEnabled
- Example value:

```
<true/>
```

Back to top

BrowserSignin

Browser sign-in settings

Supported versions:

- On Windows and macOS since 77 or later

Description

Specify whether a user can sign into Microsoft Edge with their account and use account-related services like sync and single sign on. To control the availability of sync, use the SyncDisabled policy instead.

If you set this policy to 'Disable', make sure that you also set the NonRemovableProfileEnabled policy to disabled because NonRemovableProfileEnabled disables the creation of an automatically signed in browser profile. If both policies are set, Microsoft Edge will use the 'Disable browser sign-in' policy and behave as if NonRemovableProfileEnabled is set to disabled.

If you set this policy to 'Enable', users can sign into the browser. Signing into the browser doesn't mean that sync is turned on by default; the user must separately opt-in to use this feature.

If you set this policy to 'Force', users must sign into a profile to use the browser. By default, this will allow the user to choose whether they want to sync to their account, unless sync is disabled by the domain admin or with the SyncDisabled policy. The default value of BrowserGuestModeEnabled policy is set to false.

If you don't configure this policy users can decide if they want to enable the browser sign-in option and use it as they see fit.

Policy options mapping:

- Disable (0) = Disable browser sign-in
- Enable (1) = Enable browser sign-in
- Force (2) = Force users to sign-in to use the browser

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: BrowserSignin
- GP name: Browser sign-in settings
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: BrowserSignin
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: BrowserSignin
- Example value:

```
<integer>2</integer>
```

Back to top

BrowsingDataLifetime

Browsing Data Lifetime Settings

Supported versions:

- On Windows and macOS since 89 or later

Description

Configures browsing data lifetime settings for Microsoft Edge. This policy controls the lifetime of selected browsing data. This policy has no effect if Sync is enabled. The available data types are the 'browsing_history', 'download_history', 'cookies_and_other_site_data', 'cached_images_and_files', 'password_signin', 'autofill', 'site_settings' and 'hosted_app_data'. Microsoft Edge will regularly remove data of selected types that is older than 'time_to_live_in_hours'. The deletion of expired data will happen 15 seconds after the browser starts then every hour while the browser is running.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Dictionary

Windows information and settings

Group Policy (ADMX) info

- GP unique name: BrowsingDataLifetime
- GP name: Browsing Data Lifetime Settings
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: BrowsingDataLifetime
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\BrowsingDataLifetime = [
  {
    "data_types": [
      "browsing_history"
    ],
    "time_to_live_in_hours": 24
  },
  {
    "data_types": [
      "password_signin",
      "autofill"
    ],
    "time_to_live_in_hours": 12
  }
]
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\BrowsingDataLifetime = [{"data_types": ["browsing_history"],
"time_to_live_in_hours": 24}, {"data_types": ["password_signin", "autofill"], "time_to_live_in_hours": 12}]
```

Mac information and settings

- Preference Key Name: BrowsingDataLifetime
- Example value:

```
<key>BrowsingDataLifetime</key>
<array>
  <dict>
    <key>data_types</key>
    <array>
      <string>browsing_history</string>
    </array>
    <key>time_to_live_in_hours</key>
    <integer>24</integer>
  </dict>
  <dict>
    <key>data_types</key>
    <array>
      <string>password_signin</string>
      <string>autofill</string>
    </array>
    <key>time_to_live_in_hours</key>
    <integer>12</integer>
  </dict>
</array>
```

Back to top

BuiltInDnsClientEnabled

Use built-in DNS client

Supported versions:

- On Windows and macOS since 77 or later

Description

Controls whether to use the built-in DNS client.

This policy controls which software stack is used to communicate with the DNS server: the operating system DNS client, or Microsoft Edge's built-in DNS client. This policy does not affect which DNS servers are used: if, for example, the operating system is configured to use an enterprise DNS server, that same server would be used by the built-in DNS client. It also does not control if DNS-over-HTTPS is used; Microsoft Edge always uses the built-in resolver for DNS-over-HTTPS requests. Please see the DnsOverHttpsMode policy for information on controlling DNS-over-HTTPS.

If you enable this policy, the built-in DNS client is used, if it's available.

If you disable this policy, the built-in DNS client is only used when DNS-over-HTTPS is in use.

If you don't configure this policy, the built-in DNS client is enabled by default on macOS and Android (when neither Private DNS nor VPN are enabled).

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: BuiltInDnsClientEnabled
- GP name: Use built-in DNS client
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A

- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: BuiltInDnsClientEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: BuiltInDnsClientEnabled
- Example value:

```
<true/>
```

Back to top

BuiltinCertificateVerifierEnabled

Determines whether the built-in certificate verifier will be used to verify server certificates (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 106.

Supported versions:

- On macOS since 83, until 106

Description

This policy is obsolete because it was a short-term mechanism to give enterprises more time to update their environments and report issues if they are found to be incompatible with the built-in certificate verifier.

The policy doesn't work in Microsoft Edge version 107.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Mac information and settings

- Preference Key Name: BuiltinCertificateVerifierEnabled
- Example value:

```
<false/>
```

Back to top

CECPQ2Enabled

CECPQ2 post-quantum key-agreement enabled for TLS

Supported versions:

- On Windows and macOS since 93 or later

Description

If this policy is not configured, or is set to enabled, then Microsoft Edge will follow the default rollout process for CECPQ2, a post-quantum key-agreement algorithm in TLS.

CECPQ2 results in larger TLS messages which, in very rare cases, can trigger bugs in some networking hardware. This policy can be set to False to disable CECPQ2 while networking issues are resolved.

This policy is a temporary measure and will be removed in future versions of Microsoft Edge.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: CECPQ2Enabled
- GP name: CECPQ2 post-quantum key-agreement enabled for TLS
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: CECPQ2Enabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: CECPQ2Enabled
- Example value:

```
<true/>
```

Back to top

CORSNonWildcardRequestHeadersSupport

CORS non-wildcard request header support enabled

Supported versions:

- On Windows and macOS since 97 or later

Description

This policy lets you configure support of CORS non-wildcard request headers.

Microsoft Edge version 97 introduces support for CORS non-wildcard request headers. When a script makes a cross-origin network request via fetch() and XMLHttpRequest with a script-added Authorization header, the header must be explicitly allowed by the Access-Control-Allow-Headers header in the CORS preflight response. "Explicitly" here means that the wild card symbol "*" doesn't cover the Authorization header. See https://go.microsoft.com/fwlink/?linkid=2180022 for more detail.

If you enable or don't configure the policy, Microsoft Edge will support the CORS non-wildcard request headers and behave as previously described.

If you disable this policy, Microsoft Edge will allow the wildcard symbol ("*") in the Access-Control-Allow-Headers header in the CORS preflight response to cover the Authorization header.

This policy is a temporary workaround for the new CORS non-wildcard request header feature. It's intended to be removed in the future.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: CORSNonWildcardRequestHeadersSupport
- GP name: CORS non-wildcard request header support enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: CORSNonWildcardRequestHeadersSupport
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: CORSNonWildcardRequestHeadersSupport
- Example value:

```
<true/>
```

Back to top

CertificateTransparencyEnforcementDisabledForCas

Disable Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes

Supported versions:

- On Windows and macOS since 77 or later

Description

Disables enforcement of Certificate Transparency requirements for a list of subjectPublicKeyInfo hashes.

This policy lets you disable Certificate Transparency disclosure requirements for certificate chains that contain certificates with one of the specified subjectPublicKeyInfo hashes. This allows certificates that would otherwise be untrusted because they were not properly publicly disclosed to still be used for Enterprise hosts.

To disable Certificate Transparency enforcement when this policy is set, one of the following sets of conditions

must be met:

1. The hash is of the server certificate's subjectPublicKeyInfo.
2. The hash is of a subjectPublicKeyInfo that appears in a CA certificate in the certificate chain, that CA certificate is constrained via the X.509v3 nameConstraints extension, one or more directoryName nameConstraints are present in the permittedSubtrees, and the directoryName contains an organizationName attribute.
3. The hash is of a subjectPublicKeyInfo that appears in a CA certificate in the certificate chain, the CA certificate has one or more organizationName attributes in the certificate Subject, and the server's certificate contains the same number of organizationName attributes, in the same order, and with byte-for-byte identical values.

A subjectPublicKeyInfo hash is specified by concatenating the hash algorithm name, the "/" character, and the Base64 encoding of that hash algorithm applied to the DER-encoded subjectPublicKeyInfo of the specified certificate. This Base64 encoding is the same format as an SPKI Fingerprint, as defined in RFC 7469, Section 2.4. Unrecognized hash algorithms are ignored. The only supported hash algorithm at this time is "sha256".

If you disable this policy or don't configure it, any certificate that's required to be disclosed via Certificate Transparency will be treated as untrusted if it's not disclosed according to the Certificate Transparency policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: CertificateTransparencyEnforcementDisabledForCas
- GP name: Disable Certificate Transparency enforcement for a list of subjectPublicKeyInfo hashes
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\CertificateTransparencyEnforcementDisabledForCas
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\CertificateTransparencyEnforcementDisabledForCas\1 =
"sha256/AAAAAAAAAAAAAAAAAAAAAA=="
SOFTWARE\Policies\Microsoft\Edge\CertificateTransparencyEnforcementDisabledForCas\2 =
"sha256//////////////////////w=="
```

Mac information and settings

- Preference Key Name: CertificateTransparencyEnforcementDisabledForCas
- Example value:

```
<array>
  <string>sha256/AAAAAAAAAAAAAAAAAAAAAA==</string>
  <string>sha256////////////////////w==</string>
</array>
```

Back to top

CertificateTransparencyEnforcementDisabledForLegacyCas

Disable Certificate Transparency enforcement for a list of legacy certificate authorities

Supported versions:

- On Windows and macOS since 77 or later

Description

Disables enforcing Certificate Transparency requirements for a list of legacy certificate authorities (Cas).

This policy lets you disable Certificate Transparency disclosure requirements for certificate chains that contain certificates with one of the specified subjectPublicKeyInfo hashes. This allows certificates that would otherwise be untrusted because they were not properly publicly disclosed, continue to be used for enterprise hosts.

In order for Certificate Transparency enforcement to be disabled, you must set the hash to a subjectPublicKeyInfo appearing in a CA certificate that is recognized as a legacy certificate authority (CA). A legacy CA is a CA that has been publicly trusted by default by one or more operating systems supported by Microsoft Edge.

You specify a subjectPublicKeyInfo hash by concatenating the hash algorithm name, the "/" character, and the Base64 encoding of that hash algorithm applied to the DER-encoded subjectPublicKeyInfo of the specified certificate. This Base64 encoding is the same format as an SPKI Fingerprint, as defined in RFC 7469, Section 2.4. Unrecognized hash algorithms are ignored. The only supported hash algorithm at this time is "sha256".

If you don't configure this policy, any certificate that's required to be disclosed via Certificate Transparency will be treated as untrusted if it isn't disclosed according to the Certificate Transparency policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: CertificateTransparencyEnforcementDisabledForLegacyCas
- GP name: Disable Certificate Transparency enforcement for a list of legacy certificate authorities
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\CertificateTransparencyEnforcementDisabledForLegacyCas
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\CertificateTransparencyEnforcementDisabledForLegacyCas\1 =
"sha256/AAAAAAAAAAAAAAAAAAAAAA=="
SOFTWARE\Policies\Microsoft\Edge\CertificateTransparencyEnforcementDisabledForLegacyCas\2 =
"sha256//////////////////////w=="
```

Mac information and settings

- Preference Key Name: CertificateTransparencyEnforcementDisabledForLegacyCas
- Example value:

```
<array>
  <string>sha256/AAAAAAAAAAAAAAAAAAAAAA==</string>
  <string>sha256//////////////////////w==</string>
</array>
```

Back to top

CertificateTransparencyEnforcementDisabledForUrls

Disable Certificate Transparency enforcement for specific URLs

Supported versions:

- On Windows and macOS since 77 or later

Description

Disables enforcing Certificate Transparency requirements for the listed URLs.

This policy lets you not disclose certificates for the hostnames in the specified URLs via Certificate Transparency. This lets you use certificates that would otherwise be untrusted, because they weren't properly publicly disclosed, but it makes it harder to detect mis-issued certificates for those hosts.

Form your URL pattern according to https://go.microsoft.com/fwlink/?linkid=2095322. Because certificates are valid for a given hostname, independent of the scheme, port, or path, only the hostname part of the URL is considered. Wildcard hosts are not supported.

If you don't configure this policy, any certificate that should be disclosed via Certificate Transparency is treated as untrusted if it's not disclosed.

This policy does not work as expected with file://* wildcards.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: CertificateTransparencyEnforcementDisabledForUrls
- GP name: Disable Certificate Transparency enforcement for specific URLs
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\CertificateTransparencyEnforcementDisabledForUrls
- Path (Recommended): N/A

- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\CertificateTransparencyEnforcementDisabledForUrls\1 = "contoso.com"
SOFTWARE\Policies\Microsoft\Edge\CertificateTransparencyEnforcementDisabledForUrls\2 = ".contoso.com"
```

Mac information and settings

- Preference Key Name: CertificateTransparencyEnforcementDisabledForUrls
- Example value:

```
<array>
  <string>contoso.com</string>
  <string>.contoso.com</string>
</array>
```

Back to top

ClearBrowsingDataOnExit

Clear browsing data when Microsoft Edge closes

Supported versions:

- On Windows and macOS since 78 or later

Description

Microsoft Edge doesn't clear the browsing data by default when it closes. Browsing data includes information entered in forms, passwords, and even the websites visited.

If you enable this policy, all browsing data is deleted each time Microsoft Edge closes. Note that if you enable this policy, it takes precedence over how you configured DefaultCookiesSetting

If you disable or don't configure this policy, users can configure the Clear browsing data option in Settings.

If you enable this policy, don't configure the AllowDeletingBrowserHistory or the ClearCachedImagesAndFilesOnExit policy, because they all deal with deleting browsing data. If you configure the preceding policies and this policy, all browsing data is deleted when Microsoft Edge closes, regardless of how you configured AllowDeletingBrowserHistory or ClearCachedImagesAndFilesOnExit.

To exclude cookies from being deleted on exit, configure the SaveCookiesOnExit policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ClearBrowsingDataOnExit
- GP name: Clear browsing data when Microsoft Edge closes
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ClearBrowsingDataOnExit
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ClearBrowsingDataOnExit
- Example value:

```
<true/>
```

Back to top

ClearCachedImagesAndFilesOnExit

Clear cached images and files when Microsoft Edge closes

Supported versions:

- On Windows and macOS since 83 or later

Description

Microsoft Edge doesn't clear cached images and files by default when it closes.

If you enable this policy, cached images and files will be deleted each time Microsoft Edge closes.

If you disable this policy, users cannot configure the cached images and files option in edge://settings/clearBrowsingDataOnClose.

If you don't configure this policy, users can choose whether cached images and files are cleared on exit.

If you disable this policy, don't enable the ClearBrowsingDataOnExit policy, because they both deal with deleting data. If you configure both, the ClearBrowsingDataOnExit policy takes precedence and deletes all data when Microsoft Edge closes, regardless of how you configured ClearCachedImagesAndFilesOnExit.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ClearCachedImagesAndFilesOnExit
- GP name: Clear cached images and files when Microsoft Edge closes
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ClearCachedImagesAndFilesOnExit

- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ClearCachedImagesAndFilesOnExit
- Example value:

```
<true/>
```

Back to top

ClickOnceEnabled

Allow users to open files using the ClickOnce protocol

Supported versions:

- On Windows since 78 or later

Description

Allow users to open files using the ClickOnce protocol. The ClickOnce protocol allows websites to request that the browser open files from a specific URL using the ClickOnce file handler on the user's computer or device.

If you enable this policy, users can open files using the ClickOnce protocol. This policy overrides the user's ClickOnce setting in the edge://flags/ page.

If you disable this policy, users can't open files using the ClickOnce protocol. Instead, the file will be saved to the file system using the browser. This policy overrides the user's ClickOnce setting in the edge://flags/ page.

If you don't configure this policy, users with Microsoft Edge versions before Microsoft Edge 87 can't open files using the ClickOnce protocol by default. However, they have the option to enable the use of the ClickOnce protocol with the edge://flags/ page. Users with Microsoft Edge versions 87 and later can open files using the ClickOnce protocol by default but have the option to disable the ClickOnce protocol with edge://flags/ page.

Disabling ClickOnce may prevent ClickOnce applications (.application files) from launching properly.

For more information about ClickOnce, see https://go.microsoft.com/fwlink/?linkid=2103872 and https://go.microsoft.com/fwlink/?linkid=2099880.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ClickOnceEnabled
- GP name: Allow users to open files using the ClickOnce protocol
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge

- Path (Recommended): N/A
- Value Name: ClickOnceEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

CollectionsServicesAndExportsBlockList

Block access to a specified list of services and export targets in Collections

Supported versions:

- On Windows and macOS since 86 or later

Description

List specific services and export targets that users can't access in the Collections feature in Microsoft Edge. This includes displaying additional data from Bing and exporting collections to Microsoft products or external partners.

If you enable this policy, services and export targets that match the given list are blocked.

If you don't configure this policy, no restrictions on the acceptable services and export targets are enforced.

Policy options mapping:

- pinterest_suggestions (pinterest_suggestions) = Pinterest suggestions
- collections_share (collections_share) = Sharing of Collections
- local_pdf (local_pdf) = Save local PDFs in Collections to OneDrive
- send_word (send_word) = Send collection to Microsoft Word
- send_excel (send_excel) = Send collection to Microsoft Excel
- send_onenote (send_onenote) = Send collection to Microsoft OneNote
- send_pinterest (send_pinterest) = Send collection to Pinterest

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: CollectionsServicesAndExportsBlockList
- GP name: Block access to a specified list of services and export targets in Collections
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\CollectionsServicesAndExportsBlockList

- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\CollectionsServicesAndExportsBlockList\1 = "collections_share"
SOFTWARE\Policies\Microsoft\Edge\CollectionsServicesAndExportsBlockList\2 = "local_pdf"
SOFTWARE\Policies\Microsoft\Edge\CollectionsServicesAndExportsBlockList\3 = "send_word"
SOFTWARE\Policies\Microsoft\Edge\CollectionsServicesAndExportsBlockList\4 = "send_excel"
SOFTWARE\Policies\Microsoft\Edge\CollectionsServicesAndExportsBlockList\5 = "send_onenote"
```

Mac information and settings

- Preference Key Name: CollectionsServicesAndExportsBlockList
- Example value:

```
<array>
  <string>collections_share</string>
  <string>local_pdf</string>
  <string>send_word</string>
  <string>send_excel</string>
  <string>send_onenote</string>
</array>
```

Back to top

CommandLineFlagSecurityWarningsEnabled

Enable security warnings for command-line flags

Supported versions:

- On Windows and macOS since 78 or later

Description

If disabled, this policy prevents security warnings from appearing when Microsoft Edge is launched with potentially dangerous command-line flags.

If enabled or unset, security warnings are displayed when these command-line flags are used to launch Microsoft Edge.

For example, the --disable-gpu-sandbox flag generates this warning: You're using an unsupported command-line flag: --disable-gpu-sandbox. This poses stability and security risks.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management, or macOS instances that are that are managed via MDM or joined to a domain via MCX.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: CommandLineFlagSecurityWarningsEnabled
- GP name: Enable security warnings for command-line flags

- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: CommandLineFlagSecurityWarningsEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: CommandLineFlagSecurityWarningsEnabled
- Example value:

```
<true/>
```

Back to top

ComponentUpdatesEnabled

Enable component updates in Microsoft Edge

Supported versions:

- On Windows and macOS since 77 or later

Description

If you enable or don't configure this policy, component updates are enabled in Microsoft Edge.

If you disable this policy or set it to false, component updates are disabled for all components in Microsoft Edge.

However, some components are exempt from this policy. This includes any component that doesn't contain executable code, that doesn't significantly alter the behavior of the browser, or that's critical for security. That is, updates that are deemed "critical for security" are still applied even if you disable this policy.

Examples of such components include the certificate revocation lists and security lists like tracking prevention lists.

Please note that disabling this policy can potentially prevent the Microsoft Edge developers from providing critical security fixes in a timely manner and is thus not recommended.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ComponentUpdatesEnabled
- GP name: Enable component updates in Microsoft Edge
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A

- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ComponentUpdatesEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ComponentUpdatesEnabled
- Example value:

```
<true/>
```

Back to top

ConfigureDoNotTrack

Configure Do Not Track

Supported versions:

- On Windows and macOS since 77 or later

Description

Specify whether to send Do Not Track requests to websites that ask for tracking info. Do Not Track requests let the websites you visit know that you don't want your browsing activity to be tracked. By default, Microsoft Edge doesn't send Do Not Track requests, but users can turn on this feature to send them.

If you enable this policy, Do Not Track requests are always sent to websites asking for tracking info.

If you disable this policy, requests are never sent.

If you don't configure this policy, users can choose whether to send these requests.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ConfigureDoNotTrack
- GP name: Configure Do Not Track
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ConfigureDoNotTrack

- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: ConfigureDoNotTrack
- Example value:

```
<false/>
```

Back to top

ConfigureFriendlyURLFormat

Configure the default paste format of URLs copied from Microsoft Edge, and determine if additional formats will be available to users

Supported versions:

- On Windows since 87 or later
- On macOS since 88 or later

Description

If FriendlyURLs are enabled, Microsoft Edge will compute additional representations of the URL and place them on the clipboard.

This policy configures what format will be pasted when the user pastes in external applications, or inside Microsoft Edge without the 'Paste as' context menu item.

If configured, this policy makes a choice on behalf of the user. The options in edge://settings/shareCopyPaste will be grayed out, and the options in the 'Paste As' context menu will not be available.

- Not configured = The user will be able to choose their preferred paste format. By default, this is set to the friendly URL format. The 'Paste As' menu will be available in Microsoft Edge.
- 1 = No additional formats will be stored on the clipboard. There will be no 'Paste as' context menu item in Microsoft Edge and the only format available to paste will be the plain text URL format. Effectively, the friendly URL feature will be disabled.
- 3 = The user will get a friendly URL whenever they paste into surfaces that accept rich text. The plain URL will still be available for non-rich surfaces. There will be no 'Paste As' menu in Microsoft Edge.
- 4 = (Not currently used)

The richer formats may not be well-supported in some paste destinations and/or websites. In these scenarios, the plain URL option is recommended when configuring this policy.

The recommended policy is available in Microsoft Edge 105 or later.

Policy options mapping:

- PlainText (1) = The plain URL without any extra information, such as the page's title. This is the recommended option when this policy is configured. For more information, see the description.
- TitledHyperlink (3) = Titled Hyperlink: A hyperlink that points to the copied URL, but whose visible text is the title of the destination page. This is the Friendly URL format.
- WebPreview (4) = Coming soon. If set, behaves the same as 'Plain URL'.

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ConfigureFriendlyURLFormat
- GP name: Configure the default paste format of URLs copied from Microsoft Edge, and determine if additional formats will be available to users
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ConfigureFriendlyURLFormat
- Value Type: REG_DWORD

Example value:

```
0x00000003
```

Mac information and settings

- Preference Key Name: ConfigureFriendlyURLFormat
- Example value:

```
<integer>3</integer>
```

Back to top

ConfigureKeyboardShortcuts

Configure the list of commands for which to disable keyboard shortcuts

Supported versions:

- On Windows since 101 or later

Description

Configure the list of Microsoft Edge commands for which to disable keyboard shortcuts.

See https://go.microsoft.com/fwlink/?linkid=2186950 for a list of possible commands to disable.

If you enable this policy, commands in the 'disabled' list will no longer be activated by keyboard shortcuts.

If you disable this policy, all keyboard shortcuts behave as usual.

Note: Disabling a command will only remove its shortcut mapping. Commands in the 'disabled' list will still function if accessed via browser UI.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Dictionary

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ConfigureKeyboardShortcuts
- GP name: Configure the list of commands for which to disable keyboard shortcuts
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ConfigureKeyboardShortcuts
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ConfigureKeyboardShortcuts = {
  "disabled": [
    "new_tab",
    "fullscreen"
  ]
}
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\ConfigureKeyboardShortcuts = {"disabled": ["new_tab", "fullscreen"]}
```

Back to top

ConfigureOnPremisesAccountAutoSignIn

Configure automatic sign in with an Active Directory domain account when there is no Azure AD domain account

Supported versions:

- On Windows since 81 or later

Description

Enable the use of Active Directory accounts for automatic sign in if your users' machines are Domain Joined and your environment is not hybrid joined. If you want users automatically signed in with their Azure Active Directory accounts instead, please Azure AD join (See https://go.microsoft.com/fwlink/?linkid=2118197 for more information) or hybrid join (See https://go.microsoft.com/fwlink/?linkid=2118365 for more information) your environment.

On every launch, Microsoft Edge will try to sign-in using this policy, as long as the first profile being launched isn't signed-in or an auto sign-in hasn't happened before.

If you have configured the BrowserSignin policy to disabled, this policy will not take any effect.

If you enable this policy and set it to 'SignInAndMakeDomainAccountNonRemovable', Microsoft Edge will automatically sign in users that are on domain joined machines using their Active Directory accounts.

If you set this policy to 'Disabled' or don't set it, Microsoft Edge will not automatically sign in users that are on domain joined machines with Active Directory accounts.

From Microsoft Edge 89 onwards, if there is an existing on-premises profile with RoamingProfileSupportEnabled policy disabled and machine is now hybrid joined i.e it has an Azure AD account, it will auto-upgrade the on-premises profile to Azure AD profile to get full Azure AD sync facilities.

From Microsoft Edge 93 onwards, if policy ImplicitSignInEnabled is disabled, this policy will not take any effect.

From Microsoft Edge 94 onwards, if policy OnlyOnPremisesImplicitSigninEnabled is enabled, and this policy is set to 'SignInAndMakeDomainAccountNonRemovable', it will take effect even on hybrid joined environment. Microsoft Edge will automatically sign in users using their Active Directory domain account even if there are MSA or AAD accounts.

Policy options mapping:

- Disabled (0) = Disabled
- SignInAndMakeDomainAccountNonRemovable (1) = Sign in and make domain account non-removable

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ConfigureOnPremisesAccountAutoSignIn
- GP name: Configure automatic sign in with an Active Directory domain account when there is no Azure AD domain account
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ConfigureOnPremisesAccountAutoSignIn
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

ConfigureOnlineTextToSpeech

Configure Online Text To Speech

Supported versions:

- On Windows and macOS since 77 or later

Description

Set whether the browser can leverage Online Text to Speech voice fonts, part of Azure Cognitive Services. These voice fonts are higher quality than the pre-installed system voice fonts.

If you enable or don't configure this policy, web-based applications that use the SpeechSynthesis API can use Online Text to Speech voice fonts.

If you disable this policy, the voice fonts aren't available.

Read more about this feature here: SpeechSynthesis API: https://go.microsoft.com/fwlink/?linkid=2110038 Cognitive Services: https://go.microsoft.com/fwlink/?linkid=2110141

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ConfigureOnlineTextToSpeech
- GP name: Configure Online Text To Speech
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ConfigureOnlineTextToSpeech
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ConfigureOnlineTextToSpeech
- Example value:

```
<true/>
```

Back to top

ConfigureShare

Configure the Share experience

Supported versions:

- On Windows since 83 or later
- On macOS since 93 or later

Description

If you set this policy to 'ShareAllowed' (the default), users will be able to access the Share experience from the Settings and More Menu in Microsoft Edge to share with other apps on the system.

If you set this policy to 'ShareDisallowed', users won't be able to access the Share experience. If the Share button is on the toolbar, it will also be hidden.

Policy options mapping:

- ShareAllowed (0) = Allow using the Share experience
- ShareDisallowed (1) = Don't allow using the Share experience

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ConfigureShare
- GP name: Configure the Share experience
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ConfigureShare
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ConfigureShare
- Example value:

```
<integer>1</integer>
```

Back to top

ConfigureViewInFileExplorer

Configure the View in File Explorer feature for SharePoint pages in Microsoft Edge

Supported versions:

- On Windows since 93 or later

Description

This setting allows you to configure the View in File Explorer capability for file management in SharePoint Online while using Microsoft Edge.

You will need to list the specific domains where this is allowed and list cookies needed for SharePoint authentication (rtFa and FedAuth).

Behind the scenes, the policy allows URLs with the viewinfileexplorer: scheme to open WebDAV URLs in Windows File Explorer on pages matching the list of domains and uses the cookies you specified for WebDAV authentication.

If you enable this policy, you can use the "View in File Explorer" feature on the SharePoint document libraries you list. You will need to specify the SharePoint domain and authentication cookies. See example value below.

If you disable or don't configure this policy, you cannot use the "View in File Explorer" feature on SharePoint

document libraries.

Note that while this is an available option through Microsoft Edge, rather than use the View in File Explorer option, the recommended approach to managing files and folders outside of SharePoint is to sync your SharePoint files or move or copy files in SharePoint. Sync your SharePoint files: https://go.microsoft.com/fwlink/p/?linkid=2166983 Move or copy files in SharePoint: https://go.microsoft.com/fwlink/p/?linkid=2167123

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, or Windows 10 Pro or Enterprise instances enrolled for device management.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Dictionary

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ConfigureViewInFileExplorer
- GP name: Configure the View in File Explorer feature for SharePoint pages in Microsoft Edge
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ConfigureViewInFileExplorer
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ConfigureViewInFileExplorer = [
  {
    "cookies": [
      "rtFa",
      "FedAuth"
    ],
    "domain": "contoso.sharepoint.com"
  },
  {
    "cookies": [
      "rtFa",
      "FedAuth"
    ],
    "domain": "contoso2.sharepoint.com"
  }
]
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\ConfigureViewInFileExplorer = [{"cookies": ["rtFa", "FedAuth"], "domain":
"contoso.sharepoint.com"}, {"cookies": ["rtFa", "FedAuth"], "domain": "contoso2.sharepoint.com"}]
```

Back to top

CrossOriginWebAssemblyModuleSharingEnabled

Specifies whether WebAssembly modules can be sent cross-origin (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 98.

Supported versions:

- On Windows and macOS since 95, until 98

Description

Specifies whether WebAssembly modules can be sent to another window or worker cross-origin. Cross-origin WebAssembly module sharing was deprecated as part of the efforts to deprecate document.domain, see https://github.com/mikewest/deprecating-document-domain. This policy allowed re-enabling of cross-origin WebAssembly module sharing. This policy is obsolete because it was intended to offer a longer transition period in the deprecation process.

If you enable this policy, sites can send WebAssembly modules cross-origin without restrictions.

If you disable or don't configure this policy, sites can only send WebAssembly modules to windows and workers in the same origin.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: CrossOriginWebAssemblyModuleSharingEnabled
- GP name: Specifies whether WebAssembly modules can be sent cross-origin (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: CrossOriginWebAssemblyModuleSharingEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: CrossOriginWebAssemblyModuleSharingEnabled
- Example value:

```
<true/>
```

Back to top

CustomHelpLink

Specify custom help link

Supported versions:

- On Windows and macOS since 79 or later

Description

Specify a link for the Help menu or the F1 key.

If you enable this policy, an admin can specify a link for the Help menu or the F1 key.

If you disable or don't configure this policy, the default link for the Help menu or the F1 key is used.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management, or macOS instances that are that are managed via MDM or joined to a domain via MCX.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: CustomHelpLink
- GP name: Specify custom help link
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: CustomHelpLink
- Value Type: REG_SZ

Example value:

```
"https://go.microsoft.com/fwlink/?linkid=2080734"
```

Mac information and settings

- Preference Key Name: CustomHelpLink
- Example value:

```
<string>https://go.microsoft.com/fwlink/?linkid=2080734</string>
```

Back to top

DNSInterceptionChecksEnabled

DNS interception checks enabled

Supported versions:

- On Windows and macOS since 80 or later

Description

This policy configures a local switch that can be used to disable DNS interception checks. These checks attempt to discover whether the browser is behind a proxy that redirects unknown host names.

This detection might not be necessary in an enterprise environment where the network configuration is known. It can be disabled to avoid additional DNS and HTTP traffic on start-up and each DNS configuration change.

If you enable or don't set this policy, the DNS interception checks are performed.

If you disable this policy, DNS interception checks aren't performed.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DNSInterceptionChecksEnabled
- GP name: DNS interception checks enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DNSInterceptionChecksEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: DNSInterceptionChecksEnabled
- Example value:

```
<true/>
```

Back to top

DefaultBrowserSettingEnabled

Set Microsoft Edge as default browser

Supported versions:

- On Windows 7 and macOS since 77 or later

Description

If you set this policy to True, Microsoft Edge always checks whether it's the default browser on startup and, if possible, automatically registers itself.

If you set this policy to False, Microsoft Edge is stopped from ever checking if it's the default and turns user controls off for this option.

If you don't set this policy, Microsoft Edge lets users control whether it's the default and, if not, whether user notifications should appear.

Note for Windows administrators: This policy only works for PCs running Windows 7. For later versions of

Windows, you have to deploy a "default application associations" file that makes Microsoft Edge the handler for the https and http protocols (and, optionally, the ftp protocol and file formats such as .html, .htm, .pdf, .svg, .webp). See https://go.microsoft.com/fwlink/?linkid=2094932 for more information.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultBrowserSettingEnabled
- GP name: Set Microsoft Edge as default browser
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefaultBrowserSettingEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: DefaultBrowserSettingEnabled
- Example value:

```
<true/>
```

Back to top

DefaultSearchProviderContextMenuAccessAllowed

Allow default search provider context menu search access

Supported versions:

- On Windows and macOS since 85 or later

Description

Enables the use of a default search provider on the context menu.

If you set this policy to disabled the search context menu item that relies on your default search provider and sidebar search will not be available.

If this policy is set to enabled or not set, the context menu item for your default search provider and sidebar search will be available.

The policy value is only applied when the DefaultSearchProviderEnabled policy is enabled, and is not applicable otherwise.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultSearchProviderContextMenuAccessAllowed
- GP name: Allow default search provider context menu search access
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefaultSearchProviderContextMenuAccessAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: DefaultSearchProviderContextMenuAccessAllowed
- Example value:

```
<true/>
```

Back to top

DefaultSensorsSetting

Default sensors setting

Supported versions:

- On Windows and macOS since 86 or later

Description

Set whether websites can access and use sensors such as motion and light sensors. You can completely block or allow websites to get access to sensors.

Setting the policy to 1 lets websites access and use sensors. Setting the policy to 2 denies acess to sensors.

You can override this policy for specific URL patterns by using the SensorsAllowedForUrls and SensorsBlockedForUrls policies.

If you don't configure this policy, websites can access and use sensors, and users can change this setting. This is the global default for SensorsAllowedForUrls and SensorsBlockedForUrls.

Policy options mapping:

- AllowSensors (1) = Allow sites to access sensors
- BlockSensors (2) = Do not allow any site to access sensors

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultSensorsSetting
- GP name: Default sensors setting
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefaultSensorsSetting
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: DefaultSensorsSetting
- Example value:

```
<integer>2</integer>
```

Back to top

DefaultSerialGuardSetting

Control use of the Serial API

Supported versions:

- On Windows and macOS since 86 or later

Description

Set whether websites can access serial ports. You can completely block access or ask the user each time a website wants to get access to a serial port.

Setting the policy to 3 lets websites ask for access to serial ports. Setting the policy to 2 denies access to serial ports.

You can override this policy for specific URL patterns by using the SerialAskForUrls and SerialBlockedForUrls policies.

If you don't configure this policy, by default, websites can ask users whether they can access a serial port, and users can change this setting.

Policy options mapping:

- BlockSerial (2) = Do not allow any site to request access to serial ports via the Serial API
- AskSerial (3) = Allow sites to ask for user permission to access a serial port

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultSerialGuardSetting
- GP name: Control use of the Serial API
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefaultSerialGuardSetting
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: DefaultSerialGuardSetting
- Example value:

```
<integer>2</integer>
```

Back to top

DefaultShareAdditionalOSRegionSetting

Set the default "share additional operating system region" setting

Supported versions:

- On Windows and macOS since 108 or later

Description

This policy controls the default value for the "share additional operating system region" setting in Microsoft Edge.

The "share additional operating system region" Microsoft Edge setting controls whether the OS Regional format setting will be shared with the web through the default JavaScript locale. If shared, websites will be able to query the OS Regional format using JavaScript code, for example; "Intl.DateTimeFormat().resolvedOptions().locale".

If you set this policy to "Limited", the OS Regional format will only be shared if its language part matches the Microsoft Edge display language.

If you set this policy to "Always", the OS Regional format will always be shared. This value could cause unexpected website behavior if the OS Regional format language is different from the Microsoft Edge display language. For example, if a website uses the JavaScript default locale to format dates, the names of the days and months can be displayed in one language while the surrounding text is displayed in another language.

If you set this policy to "Never", the OS Regional format will never be shared.

Example 1: In this example the OS Regional format is set to "en-GB" and the browser display language is set to "en-US". Then the OS Regional format will be shared if the policy is set to "Limited", or "Always".

Example 2: In this example the OS Regional format is set to "es-MX" and the browser display language is set to "en-US". Then the OS Regional format will be shared if the policy is set to "Always" but will not if the policy is set to "Limited",.

Policy options mapping:

- Limited (0) = Limited
- Always (1) = Always share the OS Regional format
- Never (2) = Never share the OS Regional format

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefaultShareAdditionalOSRegionSetting
- GP name: Set the default "share additional operating system region" setting
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: DefaultShareAdditionalOSRegionSetting
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: DefaultShareAdditionalOSRegionSetting
- Example value:

```
<integer>0</integer>
```

Back to top

DefinePreferredLanguages

Define an ordered list of preferred languages that websites should display in if the site supports the language

Supported versions:

- On Windows and macOS since 89 or later

Description

Configures the language variants that Microsoft Edge sends to websites as part of the Accept-Language request HTTP header and prevents users from adding, removing, or changing the order of preferred languages in Microsoft Edge settings. Users who want to change the languages Microsoft Edge displays in or offers to translate pages to will be limited to the languages configured in this policy.

If you enable this policy, websites will appear in the first language in the list that they support unless other site-specific logic is used to determine the display language. The language variants defined in this policy override the languages configured as part of the SpellcheckLanguage policy.

If you don't configure or disable this policy, Microsoft Edge sends websites the user-specified preferred languages as part of the Accept-Language request HTTP header.

For detailed information on valid language variants, see https://go.microsoft.com/fwlink/?linkid=2148854.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DefinePreferredLanguages
- GP name: Define an ordered list of preferred languages that websites should display in if the site supports the language
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DefinePreferredLanguages
- Value Type: REG_SZ

Example value:

```
"en-US,fr,es"
```

Mac information and settings

- Preference Key Name: DefinePreferredLanguages
- Example value:

```
<string>en-US,fr,es</string>
```

Back to top

DelayNavigationsForInitialSiteListDownload

Require that the Enterprise Mode Site List is available before tab navigation

Supported versions:

- On Windows since 84 or later

Description

Lets you specify whether Microsoft Edge tabs wait to navigate until the browser has downloaded the initial Enterprise Mode Site List. This setting is intended for the scenario where the browser home page should load in Internet Explorer mode, and it is important that is does so on browser first run after IE mode is enabled. If this scenario does not exist, we recommend not enabling this setting because it can negatively impact the performance of loading the home page. The setting only applies when Microsoft Edge does not have a cached Enterprise Mode Site List, such as on browser first run after IE mode is enabled.

This setting works in conjunction with: InternetExplorerIntegrationLevel is set to 'IEMode' and one of either the InternetExplorerIntegrationSiteList or the InternetExplorerIntegrationCloudSiteList policy where the list has at least one entry.

The timeout behavior of this policy can be configured with the NavigationDelayForInitialSiteListDownloadTimeout policy.

If you set this policy to 'All', when Microsoft Edge does not have a cached version of the Enterprise Mode Site List, tabs delay navigating until the browser has downloaded the site list. Sites configured to open in Internet Explorer mode by the site list will load in Internet Explorer mode, even during the initial navigation of the browser. Sites that cannot possibly be configured to open in Internet Explorer, such as any site with a scheme other than http:, https:, file:, or ftp: do not delay navigating and load immediately in Edge mode.

When used in conjunction with the InternetExplorerIntegrationCloudSiteList policy, during first launch of Microsoft Edge, there is a delay because implicit sign-in needs to finish before Microsoft Edge attempts to download the site list from the Microsoft cloud, since this requires authentication to the cloud service.

If you set this policy to 'None' or don't configure it, when Microsoft Edge does not have a cached version of the Enterprise Mode Site List, tabs will navigate immediately, and not wait for the browser to download the Enterprise Mode Site List. Sites configured to open in Internet Explorer mode by the site list will open in Microsoft Edge mode until the browser has finished downloading the Enterprise Mode Site List.

Policy options mapping:

- None (0) = None
- All (1) = All eligible navigations

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DelayNavigationsForInitialSiteListDownload
- GP name: Require that the Enterprise Mode Site List is available before tab navigation
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DelayNavigationsForInitialSiteListDownload

- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

DeleteDataOnMigration

Delete old browser data on migration

Supported versions:

- On Windows since 83 or later

Description

This policy determines whether user browsing data from Microsoft Edge Legacy will be deleted after migrating to the Microsoft Edge version 81 or later.

If you set this policy to "Enabled", all browsing data from Microsoft Edge Legacy after migrating to the Microsoft Edge version 81 or later will be deleted. This policy must be set before migrating to the Microsoft Edge version 81 or later to have any effect on existing browsing data.

If you set this policy to "Disabled", or the policy is not configured, user browsing data isn't deleted after migrating to the Microsoft Edge version 83 or later.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DeleteDataOnMigration
- GP name: Delete old browser data on migration
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DeleteDataOnMigration
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

DeveloperToolsAvailability

Control where developer tools can be used

Supported versions:

- On Windows and macOS since 77 or later

Description

Control where developer tools can be used.

If you set this policy to 'DeveloperToolsDisallowedForForceInstalledExtensions' (the default), users can access the developer tools and the JavaScript console in general, but not in the context of extensions installed by enterprise policy.

If you set this policy to 'DeveloperToolsAllowed', users can access the developer tools and the JavaScript console in all contexts, including extensions installed by enterprise policy.

If you set this policy to 'DeveloperToolsDisallowed', users can't access the developer tools or inspect website elements. Keyboard shortcuts and menu or context menu entries that open the developer tools or the JavaScript Console are disabled.

Policy options mapping:

- DeveloperToolsDisallowedForForceInstalledExtensions (0) = Block the developer tools on extensions installed by enterprise policy, allow in other contexts
- DeveloperToolsAllowed (1) = Allow using the developer tools
- DeveloperToolsDisallowed (2) = Don't allow using the developer tools

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DeveloperToolsAvailability
- GP name: Control where developer tools can be used
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DeveloperToolsAvailability
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: DeveloperToolsAvailability
- Example value:

```
<integer>2</integer>
```

Back to top

DiagnosticData

Send required and optional diagnostic data about browser usage

Supported versions:

- On Windows 7 and macOS since 86 or later

Description

This policy controls sending required and optional diagnostic data about browser usage to Microsoft.

Required diagnostic data is collected keep Microsoft Edge secure, up to date and performing as expected.

Optional diagnostic data includes data about how you use the browser, websites you visit and crash reports to Microsoft for product and service improvement.

This policy is not supported on Windows 10 devices. To control this data collection on Windows 10, IT admins must use the Windows diagnostic data group policy. This policy will either be 'Allow Telemetry' or 'Allow Diagnostic Data', depending on the version of Windows. Learn more about Windows 10 diagnostic data collection: https://go.microsoft.com/fwlink/?linkid=2099569

Use one of the following settings to configure this policy:

'Off' turns off required and optional diagnostic data collection. This option is not recommended.

'RequiredData' sends required diagnostic data but turns off optional diagnostic data collection. Microsoft Edge will send required diagnostic data to keep Microsoft Edge secure, up to date and performing as expected.

'OptionalData' sends optional diagnostic data includes data about browser usage, websites that are visited, crash reports sent to Microsoft for product and service improvement.

On Windows 7/macOS, this policy controls sending required and optional data to Microsoft.

If you don't configure this policy or disable it, Microsoft Edge will default to the user's preference.

Policy options mapping:

- Off (0) = Off (Not recommended)
- RequiredData (1) = Required data
- OptionalData (2) = Optional data

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DiagnosticData
- GP name: Send required and optional diagnostic data about browser usage
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DiagnosticData
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: DiagnosticData
- Example value:

```
<integer>2</integer>
```

Back to top

DirectInvokeEnabled

Allow users to open files using the DirectInvoke protocol

Supported versions:

- On Windows since 78 or later

Description

Allow users to open files using the DirectInvoke protocol. The DirectInvoke protocol allows websites to request that the browser open files from a specific URL using a specific file handler on the user's computer or device.

If you enable or don't configure this policy, users can open files using the DirectInvoke protocol.

If you disable this policy, users can't open files using the DirectInvoke protocol. Instead, the file will be saved to the file system.

Note: Disabling DirectInvoke may prevent certain Microsoft SharePoint Online features from working as expected.

For more information about DirectInvoke, see https://go.microsoft.com/fwlink/?linkid=2103872 and https://go.microsoft.com/fwlink/?linkid=2099871.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DirectInvokeEnabled
- GP name: Allow users to open files using the DirectInvoke protocol
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A

- Value Name: DirectInvokeEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

Disable3DAPIs

Disable support for 3D graphics APIs

Supported versions:

- On Windows and macOS since 77 or later

Description

Prevent web pages from accessing the graphics processing unit (GPU). Specifically, web pages can't access the WebGL API and plug-ins can't use the Pepper 3D API.

If you don't configure or disable this policy, it potentially allows web pages to use the WebGL API and plug-ins to use the Pepper 3D API. Microsoft Edge might, by default, still require command line arguments to be passed in order to use these APIs.

If HardwareAccelerationModeEnabled policy is set to false, the setting for 'Disable3DAPIs' policy is ignored - it's the equivalent of setting 'Disable3DAPIs' policy to true.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: Disable3DAPIs
- GP name: Disable support for 3D graphics APIs
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: Disable3DAPIs
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: Disable3DAPIs
- Example value:

```
<false/>
```

Back to top

DisableScreenshots

Disable taking screenshots

Supported versions:

- On Windows and macOS since 77 or later

Description

Controls if users can take screenshots of the browser page.

If you enable this policy, users can't take screenshots using keyboard shortcuts or extension APIs.

If you disable or don't configure this policy, users can take screenshots.

Note: Even if you disable screenshots using this policy, users might still be able to take screenshots using Web Capture within the browser or other methods outside of the browser. For example, using an operating system feature or another application.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DisableScreenshots
- GP name: Disable taking screenshots
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DisableScreenshots
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: DisableScreenshots
- Example value:

```
<true/>
```

Back to top

DiskCacheDir

Set disk cache directory

Supported versions:

- On Windows and macOS since 77 or later

Description

Configures the directory to use to store cached files.

If you enable this policy, Microsoft Edge uses the provided directory regardless of whether the user has specified the '--disk-cache-dir' flag. To avoid data loss or other unexpected errors, don't configure this policy to a volume's root directory or to a directory used for other purposes, because Microsoft Edge manages its contents.

See https://go.microsoft.com/fwlink/?linkid=2095041 for a list of variables you can use when specifying directories and paths.

If you don't configure this policy, the default cache directory is used, and users can override that default with the '--disk-cache-dir' command line flag.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DiskCacheDir
- GP name: Set disk cache directory
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DiskCacheDir
- Value Type: REG_SZ

Example value:

```
"${user_home}/Edge_cache"
```

Mac information and settings

- Preference Key Name: DiskCacheDir
- Example value:

```
<string>${user_home}/Edge_cache</string>
```

Back to top

DiskCacheSize

Set disk cache size, in bytes

Supported versions:

- On Windows and macOS since 77 or later

Description

Configures the size of the cache, in bytes, used to store files on the disk.

If you enable this policy, Microsoft Edge uses the provided cache size regardless of whether the user has specified the '--disk-cache-size' flag. The value specified in this policy isn't a hard boundary but rather a suggestion to the caching system; any value below a few megabytes is too small and will be rounded up to a reasonable minimum.

If you set the value of this policy to 0, the default cache size is used, and users can't change it.

If you don't configure this policy, the default size is used, but users can override it with the '--disk-cache-size' flag.

Note: The value specified in this policy is used as a hint to various cache subsystems in the browser. The aggregate disk usage of all caches may therefore be larger than (but within the same order of magnitude as) the value specified.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DiskCacheSize
- GP name: Set disk cache size, in bytes
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DiskCacheSize
- Value Type: REG_DWORD

Example value:

```
0x06400000
```

Mac information and settings

- Preference Key Name: DiskCacheSize
- Example value:

```
<integer>104857600</integer>
```

Back to top

DisplayCapturePermissionsPolicyEnabled

Specifies whether the display-capture permissions-policy is checked or skipped

Supported versions:

- On Windows and macOS since 95 or later

Description

The display-capture permissions-policy gates access to getDisplayMedia(), as per this spec: https://www.w3.org/TR/screen-capture/#feature-policy-integration However, if this policy is Disabled, this requirement is not enforced, and getDisplayMedia() is allowed from contexts that would otherwise be forbidden. This Enterprise policy is temporary; it's intended to be removed after Microsoft Edge version 100. It is intended to unblock Enterprise users whose application is non-spec compliant, but needs time to be fixed.

If you enable or don't configure this policy, sites can only call getDisplayMedia() from contexts which are allowlisted by the display-capture permissions-policy.

If you disable this policy, sites can call getDisplayMedia() even from contexts which are not allowlisted by the display-capture permissions policy. Note that other restrictions may still apply.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DisplayCapturePermissionsPolicyEnabled
- GP name: Specifies whether the display-capture permissions-policy is checked or skipped
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DisplayCapturePermissionsPolicyEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: DisplayCapturePermissionsPolicyEnabled
- Example value:

```
<true/>
```

Back to top

DnsOverHttpsMode

Control the mode of DNS-over-HTTPS

Supported versions:

- On Windows and macOS since 83 or later

Description

Control the mode of the DNS-over-HTTPS resolver. Note that this policy will only set the default mode for each query. The mode can be overridden for special types of queries such as requests to resolve a DNS-over-HTTPS server hostname.

The "off" mode will disable DNS-over-HTTPS.

The "automatic" mode will send DNS-over-HTTPS queries first if a DNS-over-HTTPS server is available and may fallback to sending insecure queries on error.

The "secure" mode will only send DNS-over-HTTPS queries and will fail to resolve on error.

If you don't configure this policy, the browser might send DNS-over-HTTPS requests to a resolver associated with the user's configured system resolver.

Policy options mapping:

- off (off) = Disable DNS-over-HTTPS
- automatic (automatic) = Enable DNS-over-HTTPS with insecure fallback
- secure (secure) = Enable DNS-over-HTTPS without insecure fallback

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DnsOverHttpsMode
- GP name: Control the mode of DNS-over-HTTPS
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DnsOverHttpsMode
- Value Type: REG_SZ

Example value:

```
"off"
```

Mac information and settings

- Preference Key Name: DnsOverHttpsMode
- Example value:

```
<string>off</string>
```

Back to top

DnsOverHttpsTemplates

Specify URI template of desired DNS-over-HTTPS resolver

Supported versions:

- On Windows and macOS since 83 or later

Description

The URI template of the desired DNS-over-HTTPS resolver. To specify multiple DNS-over-HTTPS resolvers, separate the corresponding URI templates with spaces.

If you set DnsOverHttpsMode to "secure" then this policy must be set and cannot be empty.

If you set DnsOverHttpsMode to "automatic" and this policy is set then the URI templates specified will be used. If you don't set this policy, then hardcoded mappings will be used to attempt to upgrade the user's current DNS resolver to a DoH resolver operated by the same provider.

If the URI template contains a dns variable, requests to the resolver will use GET; otherwise requests will use POST.

Incorrectly formatted templates will be ignored.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DnsOverHttpsTemplates
- GP name: Specify URI template of desired DNS-over-HTTPS resolver
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DnsOverHttpsTemplates
- Value Type: REG_SZ

Example value:

```
"https://dns.example.net/dns-query{?dns}"
```

Mac information and settings

- Preference Key Name: DnsOverHttpsTemplates
- Example value:

```
<string>https://dns.example.net/dns-query{?dns}</string>
```

Back to top

DoNotSilentlyBlockProtocolsFromOrigins

Define a list of protocols that can not be silently blocked by anti-flood protection

Supported versions:

- On Windows and macOS since 99 or later

Description

Allows you to create a list of protocols, and for each protocol an associated list of allowed origin patterns. These origins won't be silently blocked from launching an external application by anti-flood protection. The trailing separator shouldn't be included when listing the protocol. For example, list "skype" instead of "skype:" or "skype://".

If you configure this policy, a protocol will only be permitted to bypass being silently blocked by anti-flood protection if:

- the protocol is listed
- the origin of the site trying to launch the protocol matches one of the origin patterns in that protocol's allowed_origins list.

If either condition is false, the external protocol launch may be blocked by anti-flood protection.

If you don't configure this policy, no protocols can bypass being silently blocked.

The origin matching patterns use a similar format to those for the URLBlocklist policy, that are documented at https://go.microsoft.com/fwlink/?linkid=2095322.

However, origin matching patterns for this policy cannot contain "/path" or "@query" elements. Any pattern that does contain a "/path" or "@query" element will be ignored.

This policy doesn't work as expected with file://* wildcards.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Dictionary

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DoNotSilentlyBlockProtocolsFromOrigins
- GP name: Define a list of protocols that can not be silently blocked by anti-flood protection
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DoNotSilentlyBlockProtocolsFromOrigins
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\DoNotSilentlyBlockProtocolsFromOrigins = [
  {
    "allowed_origins": [
      "example.com",
      "http://www.example.com:8080"
    ],
    "protocol": "spotify"
  },
  {
    "allowed_origins": [
      "https://example.com",
      "https://.mail.example.com"
    ],
    "protocol": "msteams"
  },
  {
    "allowed_origins": [
      "*"
    ],
    "protocol": "msoutlook"
  }
]
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\DoNotSilentlyBlockProtocolsFromOrigins = [{"allowed_origins":
["example.com", "http://www.example.com:8080"], "protocol": "spotify"}, {"allowed_origins":
["https://example.com", "https://.mail.example.com"], "protocol": "msteams"}, {"allowed_origins": ["*"],
"protocol": "msoutlook"}]
```

Mac information and settings

- Preference Key Name: DoNotSilentlyBlockProtocolsFromOrigins
- Example value:

```
<key>DoNotSilentlyBlockProtocolsFromOrigins</key>
<array>
  <dict>
    <key>allowed_origins</key>
    <array>
      <string>example.com</string>
      <string>http://www.example.com:8080</string>
    </array>
    <key>protocol</key>
    <string>spotify</string>
  </dict>
  <dict>
    <key>allowed_origins</key>
    <array>
      <string>https://example.com</string>
      <string>https://.mail.example.com</string>
    </array>
    <key>protocol</key>
    <string>msteams</string>
  </dict>
  <dict>
    <key>allowed_origins</key>
    <array>
      <string>*</string>
    </array>
    <key>protocol</key>
    <string>msoutlook</string>
  </dict>
</array>
```

Back to top

DoubleClickCloseTabEnabled

Double Click feature in Microsoft Edge enabled (only available in China)

Supported versions:

- On Windows and macOS since 104 or later

Description

This policy lets you configure the double click feature in Microsoft Edge.

Double Click lets users close a tab by double clicking the left mouse button.

If you enable or don't configure this policy, you can use the double click feature to close a tab on Microsoft Edge to start using this feature.

If you disable this policy, you can't use the double click feature in Microsoft Edge.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DoubleClickCloseTabEnabled
- GP name: Double Click feature in Microsoft Edge enabled (only available in China)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: DoubleClickCloseTabEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: DoubleClickCloseTabEnabled
- Example value:

```
<true/>
```

Back to top

DownloadDirectory

Set download directory

Supported versions:

- On Windows and macOS since 77 or later

Description

Configures the directory to use when downloading files.

If you enable this policy, Microsoft Edge uses the provided directory regardless of whether the user has specified one or chosen to be prompted for download location every time. See https://go.microsoft.com/fwlink/?linkid=2095041 for a list of variables that can be used.

If you disable or don't configure this policy, the default download directory is used, and the user can change it.

If you set an invalid path, Microsoft Edge will default to the user's default download directory.

If the folder specified by the path doesn't exist, the download will trigger a prompt that asks the user where they want to save their download.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DownloadDirectory
- GP name: Set download directory
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: DownloadDirectory
- Value Type: REG_SZ

Example value:

```
"\n      Linux-based OSes (including Mac): /home/${user_name}/Downloads\n      Windows:
C:\\Users\\${user_name}\\Downloads"
```

Mac information and settings

- Preference Key Name: DownloadDirectory
- Example value:

```
<string>
      Linux-based OSes (including Mac): /home/${user_name}/Downloads
      Windows: C:\Users\${user_name}\Downloads</string>
```

Back to top

DownloadRestrictions

Allow download restrictions

Supported versions:

- On Windows and macOS since 77 or later

Description

Configures the type of downloads that Microsoft Edge completely blocks, without letting users override the

security decision.

Set 'BlockDangerousDownloads' to allow all downloads except for those that carry Microsoft Defender SmartScreen warnings of known dangerous downloads or that have dangerous file type extensions.

Set 'BlockPotentiallyDangerousDownloads' to allow all downloads except for those that carry Microsoft Defender SmartScreen warnings of potentially dangerous or unwanted downloads or that have dangerous file type extensions.

Set 'BlockAllDownloads' to block all downloads.

Set 'BlockMaliciousDownloads' to allow all downloads except for those that carry Microsoft Defender SmartScreen warnings of known malicious downloads.

If you don't configure this policy or set the 'DefaultDownloadSecurity' option, the downloads go through the usual security restrictions based on Microsoft Defender SmartScreen analysis results.

Note that these restrictions apply to downloads from web page content, as well as the 'download link...' context menu option. These restrictions don't apply to saving or downloading the currently displayed page, nor do they apply to the Save as PDF option from the printing options.

See https://go.microsoft.com/fwlink/?linkid=2094934 for more info on Microsoft Defender SmartScreen.

Policy options mapping:

- DefaultDownloadSecurity (0) = No special restrictions
- BlockDangerousDownloads (1) = Block malicious downloads and dangerous file types
- BlockPotentiallyDangerousDownloads (2) = Block potentially dangerous or unwanted downloads and dangerous file types
- BlockAllDownloads (3) = Block all downloads
- BlockMaliciousDownloads (4) = Block malicious downloads

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: DownloadRestrictions
- GP name: Allow download restrictions
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: DownloadRestrictions
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: DownloadRestrictions
- Example value:

```
<integer>2</integer>
```

Back to top

EdgeAssetDeliveryServiceEnabled

Allow features to download assets from the Asset Delivery Service

Supported versions:

- On Windows and macOS since 101 or later

Description

The Asset Delivery Service is a general pipeline used to deliver assets to the Microsoft Edge Clients. These assets can be config files or Machine Learning models that power the features that use this service.

If you enable or don't configure this policy, features can download assets from the Asset Delivery Service.

If you disable this policy, features won't be able to download assets needed for them to run correctly.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EdgeAssetDeliveryServiceEnabled
- GP name: Allow features to download assets from the Asset Delivery Service
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: EdgeAssetDeliveryServiceEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: EdgeAssetDeliveryServiceEnabled
- Example value:

```
<false/>
```

Back to top

EdgeCollectionsEnabled

Enable the Collections feature

Supported versions:

- On Windows and macOS since 78 or later

Description

Lets you allow users to access the Collections feature, where they can collect, organize, share, and export content more efficiently and with Office integration.

If you enable or don't configure this policy, users can access and use the Collections feature in Microsoft Edge.

If you disable this policy, users can't access and use Collections in Microsoft Edge.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EdgeCollectionsEnabled
- GP name: Enable the Collections feature
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: EdgeCollectionsEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: EdgeCollectionsEnabled
- Example value:

```
<true/>
```

Back to top

EdgeDiscoverEnabled

Discover feature In Microsoft Edge (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 105.

Supported versions:

- On Windows and macOS since 97, until 105

Description

This policy doesn't work because Discover is now contained within the Edge Sidebar and can be managed using the HubsSidebarEnabled policy.

This policy lets you configure the Discover feature in Microsoft Edge.

Working in the background when enabled, this feature sends URLs to Microsoft Bing to search for related recommendations.

If you enable or don't configure this policy, you can use the Discover button on Microsoft Edge to start using this feature.

If you disable this policy, you can't use the Discover feature in Microsoft Edge.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EdgeDiscoverEnabled
- GP name: Discover feature In Microsoft Edge (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: EdgeDiscoverEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: EdgeDiscoverEnabled
- Example value:

```
<true/>
```

Back to top

EdgeEDropEnabled

Enable Drop feature in Microsoft Edge

Supported versions:

- On Windows and macOS since 104 or later

Description

This policy lets you configure the Drop feature in Microsoft Edge.

Drop lets users send messages or files to themselves.

If you enable or don't configure this policy, you can use the Drop feature in Microsoft Edge.

If you disable this policy, you can't use the Drop feature in Microsoft Edge.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EdgeEDropEnabled
- GP name: Enable Drop feature in Microsoft Edge
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: EdgeEDropEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: EdgeEDropEnabled
- Example value:

```
<true/>
```

Back to top

EdgeEnhanceImagesEnabled

Enhance images enabled

Supported versions:

- On Windows and macOS since 97 or later

Description

Set whether Microsoft Edge can automatically enhance images to show you sharper images with better color, lighting, and contrast.

If you enable this policy or don't configure the policy, Microsoft Edge will automatically enhance images on specific web applications.

If you disable this policy, Microsoft Edge will not enhance images.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EdgeEnhanceImagesEnabled
- GP name: Enhance images enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: EdgeEnhanceImagesEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: EdgeEnhanceImagesEnabled
- Example value:

```
<true/>
```

Back to top

EdgeFollowEnabled

Enable Follow service in Microsoft Edge

Supported versions:

- On Windows and macOS since 98 or later

Description

Allows the Microsoft Edge browser to enable Follow service and apply it to users.

Users can use the Follow an influencer, site, or topic in Microsoft Edge..

If you enable or don't configure this policy, Follow in Microsoft Edge can be applied.

If you disable this policy, Microsoft Edge will not communicate with Follow service to provide the follow feature.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EdgeFollowEnabled
- GP name: Enable Follow service in Microsoft Edge
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: EdgeFollowEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: EdgeFollowEnabled
- Example value:

```
<true/>
```

Back to top

EdgeShoppingAssistantEnabled

Shopping in Microsoft Edge Enabled

Supported versions:

- On Windows and macOS since 87 or later

Description

This policy lets users compare the prices of a product they are looking at, get coupons or rebates from the website they're on, auto-apply coupons and help checkout faster using autofill data.

If you enable or don't configure this policy, shopping features such as price comparison, coupons, rebates and express checkout will be automatically applied for retail domains. Coupons for the current retailer and prices from other retailers will be fetched from a server.

If you disable this policy shopping features such as price comparison, coupons, rebates and express checkout will not be automatically found for retail domains.

Starting in version 90.0.818.56, the behavior of the messaging letting users know that there is a coupon, rebate, price comparison or price history available on shopping domains is also done through a horizontal banner below the address bar. Previously this messaging was done on the address bar.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EdgeShoppingAssistantEnabled
- GP name: Shopping in Microsoft Edge Enabled

- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: EdgeShoppingAssistantEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: EdgeShoppingAssistantEnabled
- Example value:

```
<true/>
```

Back to top

EditFavoritesEnabled

Allows users to edit favorites

Supported versions:

- On Windows and macOS since 77 or later

Description

Enable this policy to let users add, remove, and modify favorites. This is the default behavior if you don't configure the policy.

Disable this policy to stop users from adding, removing, or modifying favorites. They can still use existing favorites.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EditFavoritesEnabled
- GP name: Allows users to edit favorites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: EditFavoritesEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: EditFavoritesEnabled
- Example value:

```
<false/>
```

Back to top

EnableDeprecatedWebPlatformFeatures

Re-enable deprecated web platform features for a limited time (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 86.

Supported versions:

- On Windows and macOS since 77, until 86

Description

This policy is obsolete because dedicated web platform policies are now used to manage individual web platform feature deprecations.

Specify a list of deprecated web platform features to temporarily re-enable.

This policy lets you re-enable deprecated web platform features for a limited time. Features are identified by a string tag.

If you don't configure this policy, if the list is empty, or if a feature doesn't match one of the supported string tags, all deprecated web platform features remain disabled.

While the policy itself is supported on the above platforms, the feature it's enabling might not be available on all of those platforms. Not all deprecated Web Platform features can be re-enabled. Only those explicitly listed below can be re-enabled, and only for a limited period of time, which differs per feature. You can review the intent behind the Web Platform feature changes at https://bit.ly/blinkintents.

The general format of the string tag is [DeprecatedFeatureName]_EffectiveUntil[yyyymmdd].

Policy options mapping:

- ExampleDeprecatedFeature (ExampleDeprecatedFeature_EffectiveUntil20080902) = Enable ExampleDeprecatedFeature API through 2008/09/02

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EnableDeprecatedWebPlatformFeatures
- GP name: Re-enable deprecated web platform features for a limited time (obsolete)

- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\EnableDeprecatedWebPlatformFeatures
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\EnableDeprecatedWebPlatformFeatures\1 =
"ExampleDeprecatedFeature_EffectiveUntil20080902"
```

Mac information and settings

- Preference Key Name: EnableDeprecatedWebPlatformFeatures
- Example value:

```
<array>
  <string>ExampleDeprecatedFeature_EffectiveUntil20080902</string>
</array>
```

Back to top

EnableDomainActionsDownload

Enable Domain Actions Download from Microsoft (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 84.

Supported versions:

- On Windows and macOS since 77, until 84

Description

This policy doesn't work because conflicting states should be avoided. This policy was used to enable/disable download of the domain actions list, but it didn't always achieve the desired state. The Experimentation and Configuration Service, which handles the download, has its own policy to configure what is downloaded from the service. Use the ExperimentationAndConfigurationServiceControl policy instead.

In Microsoft Edge, Domain Actions represent a series of compatibility features that help the browser work correctly on the web.

Microsoft keeps a list of actions to take on certain domains for compatibility reasons. For example, the browser may override the User Agent string on a website if that website is broken due to the new User Agent string on Microsoft Edge. Each of these actions is intended to be temporary while Microsoft tries to resolve the issue with the site owner.

When the browser starts up and then periodically afterwards, the browser will contact the Experimentation and Configuration Service that contains the most up to date list of compatibility actions to perform. This list is saved locally after it is first retrieved so that subsequent requests will only update the list if the server's copy has changed.

If you enable this policy, the list of Domain Actions will continue to be downloaded from the Experimentation and Configuration Service.

If you disable this policy, the list of Domain Actions will no longer be downloaded from the Experimentation and Configuration Service.

If you don't configure this policy, the list of Domain Actions will continue to be downloaded from the Experimentation and Configuration Service.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EnableDomainActionsDownload
- GP name: Enable Domain Actions Download from Microsoft (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: EnableDomainActionsDownload
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: EnableDomainActionsDownload
- Example value:

```
<true/>
```

Back to top

EnableOnlineRevocationChecks

Enable online OCSP/CRL checks

Supported versions:

- On Windows and macOS since 77 or later

Description

Online revocation checks don't provide a significant security benefit and are disabled by default.

If you enable this policy, Microsoft Edge will perform soft-fail, online OCSP/CRL checks. "Soft fail" means that if the revocation server can't be reached, the certificate will be considered valid.

If you disable the policy or don't configure it, Microsoft Edge won't perform online revocation checks.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No

- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EnableOnlineRevocationChecks
- GP name: Enable online OCSP/CRL checks
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: EnableOnlineRevocationChecks
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: EnableOnlineRevocationChecks
- Example value:

```
<false/>
```

Back to top

EnableSha1ForLocalAnchors

Allow certificates signed using SHA-1 when issued by local trust anchors (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 91.

Supported versions:

- On Windows and macOS since 85, until 91

Description

When this setting is enabled, Microsoft Edge allows connections secured by SHA-1 signed certificates so long as the the certificate chains to a locally-installed root certificate and is otherwise valid.

Note that this policy depends on the operating system (OS) certificate verification stack allowing SHA-1 signatures. If an OS update changes the OS handling of SHA-1 certificates, this policy might no longer have effect. Further, this policy is intended as a temporary workaround to give enterprises more time to move away from SHA-1. This policy will be removed in Microsoft Edge 92 releasing in mid 2021.

If you don't set this policy or set it to false, or the SHA-1 certificate chains to a publicly trusted certificate root, then Microsoft Edge won't allow certificates signed by SHA-1.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management, or macOS instances that are that are managed via MDM or joined to a domain via MCX.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EnableSha1ForLocalAnchors
- GP name: Allow certificates signed using SHA-1 when issued by local trust anchors (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: EnableSha1ForLocalAnchors
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: EnableSha1ForLocalAnchors
- Example value:

```
<false/>
```

Back to top

EncryptedClientHelloEnabled

TLS Encrypted ClientHello Enabled

Supported versions:

- On Windows and macOS since 108 or later

Description

Encrypted ClientHello (ECH) is an extension to TLS that encrypts the sensitive fields of ClientHello to improve privacy.

If ECH is enabled, Microsoft Edge might or might not use ECH depending on server support, the availability of the HTTPS DNS record, or the rollout status.

If you enable or do not configure this policy, Microsoft Edge will follow the default rollout process for ECH.

If this policy is disabled, Microsoft Edge will not enable ECH.

Because ECH is an evolving protocol, Microsoft Edge's implementation is subject to change.

As such, this policy is a temporary measure to control the initial experimental implementation. It will be replaced with final controls as the protocol finalizes.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No

- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EncryptedClientHelloEnabled
- GP name: TLS Encrypted ClientHello Enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: EncryptedClientHelloEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: EncryptedClientHelloEnabled
- Example value:

```
<true/>
```

Back to top

EnhanceSecurityMode

Enhance the security state in Microsoft Edge

Supported versions:

- On Windows and macOS since 98 or later

Description

This policy lets you enhance the security state in Microsoft Edge.

If you set this policy to 'StandardMode', the enhanced mode will be turned off and Microsoft Edge will fallback to its standard security mode.

If you set this policy to 'BalancedMode', the security state will be in balanced mode.

If you set this policy to 'StrictMode', the security state will be in strict mode.

If you set this policy to 'BasicMode', the security state will be in basic mode.

Note: Sites that use WebAssembly (WASM) are not currently supported when EnhanceSecurityMode is enabled. If you require access to a site that uses WASM, consider adding it to your exception list as described in https://go.microsoft.com/fwlink/?linkid=2183321.

For detailed information about Enhanced Security Mode, see https://go.microsoft.com/fwlink/?linkid=2185895

Policy options mapping:

- StandardMode (0) = Standard mode

- BalancedMode (1) = Balanced mode
- StrictMode (2) = Strict mode
- BasicMode (3) = Basic mode

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EnhanceSecurityMode
- GP name: Enhance the security state in Microsoft Edge
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: EnhanceSecurityMode
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: EnhanceSecurityMode
- Example value:

```
<integer>0</integer>
```

Back to top

EnhanceSecurityModeBypassIntranet

Enhanced Security Mode configuration for Intranet zone sites

Supported versions:

- On Windows since 107 or later

Description

Microsoft Edge will apply Enhanced Security Mode on Intranet zone sites by default. This may lead to Intranet zone sites acting in an unexpected manner.

If you enable this policy, Microsoft Edge won't apply Enhanced Security Mode on Intranet zone sites.

If you disable or don't configure this policy, Microsoft Edge will apply Enhanced Security Mode on Intranet zone sites.

For detailed information about Enhanced Security Mode, see https://go.microsoft.com/fwlink/?linkid=2185895

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EnhanceSecurityModeBypassIntranet
- GP name: Enhanced Security Mode configuration for Intranet zone sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: EnhanceSecurityModeBypassIntranet
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

EnhanceSecurityModeBypassListDomains

Configure the list of domains for which enhance security mode will not be enforced

Supported versions:

- On Windows and macOS since 98 or later

Description

Configure the list of enhance security trusted domains. This means that enhance security mode will not be enforced when loading the sites in trusted domains.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EnhanceSecurityModeBypassListDomains
- GP name: Configure the list of domains for which enhance security mode will not be enforced
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\EnhanceSecurityModeBypassListDomains
- Path (Recommended): N/A

- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\EnhanceSecurityModeBypassListDomains\1 = "mydomain.com"
SOFTWARE\Policies\Microsoft\Edge\EnhanceSecurityModeBypassListDomains\2 = "myuniversity.edu"
```

Mac information and settings

- Preference Key Name: EnhanceSecurityModeBypassListDomains
- Example value:

```
<array>
  <string>mydomain.com</string>
  <string>myuniversity.edu</string>
</array>
```

Back to top

EnhanceSecurityModeEnforceListDomains

Configure the list of domains for which enhance security mode will always be enforced

Supported versions:

- On Windows and macOS since 98 or later

Description

Configure the list of enhance security untrusted domains. This means that enhance security mode will always be enforced when loading the sites in untrusted domains.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EnhanceSecurityModeEnforceListDomains
- GP name: Configure the list of domains for which enhance security mode will always be enforced
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\EnhanceSecurityModeEnforceListDomains
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\EnhanceSecurityModeEnforceListDomains\1 = "mydomain.com"
SOFTWARE\Policies\Microsoft\Edge\EnhanceSecurityModeEnforceListDomains\2 = "myuniversity.edu"
```

Mac information and settings

- Preference Key Name: EnhanceSecurityModeEnforceListDomains
- Example value:

```
<array>
  <string>mydomain.com</string>
  <string>myuniversity.edu</string>
</array>
```

Back to top

EnterpriseHardwarePlatformAPIEnabled

Allow managed extensions to use the Enterprise Hardware Platform API

Supported versions:

- On Windows and macOS since 78 or later

Description

When this policy is set to enabled, extensions installed by enterprise policy are allowed to use the Enterprise Hardware Platform API. When this policy is set to disabled or isn't set, no extensions are allowed to use the Enterprise Hardware Platform API. This policy also applies to component extensions.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EnterpriseHardwarePlatformAPIEnabled
- GP name: Allow managed extensions to use the Enterprise Hardware Platform API
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: EnterpriseHardwarePlatformAPIEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: EnterpriseHardwarePlatformAPIEnabled
- Example value:

```
<true/>
```

Back to top

EnterpriseModeSiteListManagerAllowed

Allow access to the Enterprise Mode Site List Manager tool

Supported versions:

- On Windows since 86 or later

Description

Allows you to set whether Enterprise Mode Site List Manager is available to users.

If you enable this policy, users can see the Enterprise Mode Site List Manager nav button on edge://compat page, navigate to the tool and use it.

If you disable or don't configure this policy, users won't see the Enterprise Mode Site List Manager nav button and won't be able to use it.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EnterpriseModeSiteListManagerAllowed
- GP name: Allow access to the Enterprise Mode Site List Manager tool
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: EnterpriseModeSiteListManagerAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

EventPathEnabled

Re-enable the Event.path API until Microsoft Edge version 115

Supported versions:

- On Windows and macOS since 107, until 115

Description

Starting in Microsoft Edge version 109, the non-standard API Event.path will be removed to improve web compatibility. This policy re-enables the API until version 115.

If you enable this policy, the Event.path API will be available.

If you disable this policy, the Event.path API will be unavailable.

If this policy is not set, the Event.path API will be in the following default states: available before version 109, and unavailable in version 109 to version 114.

This policy will be made obsolete after Microsoft Edge version 115.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: EventPathEnabled
- GP name: Re-enable the Event.path API until Microsoft Edge version 115
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: EventPathEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: EventPathEnabled
- Example value:

```
<true/>
```

Back to top

ExemptDomainFileTypePairsFromFileTypeDownloadWarnings

Disable download file type extension-based warnings for specified file types on domains (deprecated)

> DEPRECATED: This policy is deprecated. It is currently supported but will become obsolete in a future release.

Supported versions:

- On Windows and macOS since 85 or later

Description

This policy is being deprecated in favor of ExemptFileTypeDownloadWarnings because of a type mismatch that caused errors in Mac. This policy will be made obsolete after version 108. If you set both policies, values from this policy will be overridden if they're set differently in ExemptFileTypeDownloadWarnings.

You can enable this policy to create a dictionary of file type extensions with a corresponding list of domains that will be exempted from file type extension-based download warnings. This lets enterprise administrators block file type extension-based download warnings for files that are associated with a listed domain. For example, if the "jnlp" extension is associated with "website1.com", users would not see a warning when downloading "jnlp" files from "website1.com", but see a download warning when downloading "jnlp" files from "website2.com".

Files with file type extensions specified for domains identified by this policy will still be subject to non-file type extension-based security warnings such as mixed-content download warnings and Microsoft Defender SmartScreen warnings.

If you disable this policy or don't configure it, file types that trigger extension-based download warnings will show warnings to the user.

If you enable this policy:

- The URL pattern should be formatted according to https://go.microsoft.com/fwlink/?linkid=2095322.
- The file type extension entered must be in lower-cased ASCII. The leading separator should not be included when listing the file type extension, so list "jnlp" should be used instead of ".jnlp".

Example:

The following example value would prevent file type extension-based download warnings on swf, exe, and jnlp extensions for *.contoso.com domains. It will show the user a file type extension-based download warning on any other domain for exe and jnlp files, but not for swf files.

[{ "file_extension": "jnlp", "domains": ["contoso.com"] }, { "file_extension": "exe", "domains": ["contoso.com"] }, { "file_extension": "swf", "domains": ["*"] }]

Note that while the preceding example shows the suppression of file type extension-based download warnings for "swf" files for all domains, applying suppression of such warnings for all domains for any dangerous file type extension is not recommended due to security concerns. It is shown in the example merely to demonstrate the ability to do so.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ExemptDomainFileTypePairsFromFileTypeDownloadWarnings
- GP name: Disable download file type extension-based warnings for specified file types on domains (deprecated)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\ExemptDomainFileTypePairsFromFileTypeDownloadWarnings
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ExemptDomainFileTypePairsFromFileTypeDownloadWarnings\1 =
{"file_extension": "jnlp", "domains": ["https://contoso.com", "contoso2.com"]}
SOFTWARE\Policies\Microsoft\Edge\ExemptDomainFileTypePairsFromFileTypeDownloadWarnings\2 =
{"file_extension": "swf", "domains": ["*"]}
```

Mac information and settings

- Preference Key Name: ExemptDomainFileTypePairsFromFileTypeDownloadWarnings
- Example value:

```
<array>
  <string>{'file_extension': 'jnlp', 'domains': ['https://contoso.com', 'contoso2.com']}</string>
  <string>{'file_extension': 'swf', 'domains': ['*']}</string>
</array>
```

Back to top

ExemptFileTypeDownloadWarnings

Disable download file type extension-based warnings for specified file types on domains

Supported versions:

- On Windows and macOS since 105 or later

Description

You can enable this policy to create a dictionary of file type extensions with a corresponding list of domains that will be exempted from file type extension-based download warnings. This lets enterprise administrators block file type extension-based download warnings for files that are associated with a listed domain. For example, if the "jnlp" extension is associated with "website1.com", users would not see a warning when downloading "jnlp" files from "website1.com", but see a download warning when downloading "jnlp" files from "website2.com".

Files with file type extensions specified for domains identified by this policy will still be subject to non-file type extension-based security warnings such as mixed-content download warnings and Microsoft Defender SmartScreen warnings.

If you disable this policy or don't configure it, file types that trigger extension-based download warnings will show warnings to the user.

If you enable this policy:

- The URL pattern should be formatted according to https://go.microsoft.com/fwlink/?linkid=2095322.
- The file type extension entered must be in lower-cased ASCII. The leading separator should not be included when listing the file type extension, so list "jnlp" should be used instead of ".jnlp".

Example:

The following example value would prevent file type extension-based download warnings on swf, exe, and jnlp extensions for *.contoso.com domains. It will show the user a file type extension-based download warning on any other domain for exe and jnlp files, but not for swf files.

[{ "file_extension": "jnlp", "domains": ["contoso.com"] }, { "file_extension": "exe", "domains": ["contoso.com"] }, { "file_extension": "swf", "domains": ["*"] }]

Note that while the preceding example shows the suppression of file type extension-based download warnings for "swf" files for all domains, applying suppression of such warnings for all domains for any dangerous file type extension is not recommended due to security concerns. It is shown in the example merely to demonstrate the ability to do so.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Dictionary

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ExemptFileTypeDownloadWarnings
- GP name: Disable download file type extension-based warnings for specified file types on domains
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ExemptFileTypeDownloadWarnings
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ExemptFileTypeDownloadWarnings = [
  {
    "domains": [
      "https://contoso.com",
      "contoso2.com"
    ],
    "file_extension": "jnlp"
  },
  {
    "domains": [
      "*"
    ],
    "file_extension": "swf"
  }
]
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\ExemptFileTypeDownloadWarnings = [{"domains": ["https://contoso.com",
"contoso2.com"], "file_extension": "jnlp"}, {"domains": ["*"], "file_extension": "swf"}]
```

Mac information and settings

- Preference Key Name: ExemptFileTypeDownloadWarnings
- Example value:

```
<key>ExemptFileTypeDownloadWarnings</key>
<array>
  <dict>
    <key>domains</key>
    <array>
      <string>https://contoso.com</string>
      <string>contoso2.com</string>
    </array>
    <key>file_extension</key>
    <string>jnlp</string>
  </dict>
  <dict>
    <key>domains</key>
    <array>
      <string>*</string>
    </array>
    <key>file_extension</key>
    <string>swf</string>
  </dict>
</array>
```

Back to top

ExperimentationAndConfigurationServiceControl

Control communication with the Experimentation and Configuration Service

Supported versions:

- On Windows and macOS since 77 or later

Description

The Experimentation and Configuration Service is used to deploy Experimentation and Configuration payloads to the client.

Experimentation payload consists of a list of early in development features that Microsoft is enabling for testing and feedback.

Configuration payload consists of a list of recommended settings that Microsoft wants to deploy to optimize the user experience.

Configuration payload may also contain a list of actions to take on certain domains for compatibility reasons. For example, the browser may override the User Agent string on a website if that website is broken. Each of these actions is intended to be temporary while Microsoft tries to resolve the issue with the site owner.

If you set this policy to 'FullMode', the full payload is downloaded from the Experimentation and Configuration Service. This includes both the experimentation and configuration payloads.

If you set this policy to 'ConfigurationsOnlyMode', only the configuration payload is downloaded.

If you set this policy to 'RestrictedMode', the communication with the Experimentation and Configuration Service is stopped completely. Microsoft does not recommend this setting.

If you don't configure this policy on a managed device, the behavior on Beta and Stable channels is the same as the 'ConfigurationsOnlyMode'. On Canary and Dev channels the behavior is the same as 'FullMode'.

If you don't configure this policy on an unmanaged device, the behavior is the same as the 'FullMode'.

Policy options mapping:

- FullMode (2) = Retrieve configurations and experiments
- ConfigurationsOnlyMode (1) = Retrieve configurations only
- RestrictedMode (0) = Disable communication with the Experimentation and Configuration Service

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ExperimentationAndConfigurationServiceControl
- GP name: Control communication with the Experimentation and Configuration Service
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ExperimentationAndConfigurationServiceControl
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: ExperimentationAndConfigurationServiceControl
- Example value:

```
<integer>2</integer>
```

Back to top

ExplicitlyAllowedNetworkPorts

Explicitly allowed network ports

Supported versions:

- On Windows and macOS since 91 or later

Description

There is a list of restricted ports built into Microsoft Edge. Connections to these ports will fail. This policy allows bypassing that list. The set of ports is defined as a comma-separated list that outgoing connections should be permitted on.

Ports are restricted to prevent Microsoft Edge from being used as a vector to exploit various network vulnerabilities. Setting this policy may expose your network to attacks. This policy is intended as a temporary workaround for error code "ERR_UNSAFE_PORT" while migrating a service running on a blocked port to a standard port (for example port 80 or 443).

Malicious websites can easily detect that this policy is set, and for which ports, then use that information to target attacks.

Each port listed in this policy is labeled with a date that it can be unblocked until. After that date the port will be restricted regardless of if it's specified by the value of this policy.

Leaving the value empty or unset means that all restricted ports will be blocked. Invalid port values set through this policy will be ignored while valid ones will still be applied.

This policy overrides the "--explicitly-allowed-ports" command-line option.

Policy options mapping:

- 554 (554) = port 554 (can be unblocked until 2021/10/15)
- 10080 (10080) = port 10080 (can be unblocked until 2022/04/01)
- 6566 (6566) = port 6566 (can be unblocked until 2021/10/15)
- 989 (989) = port 989 (can be unblocked until 2022/02/01)
- 990 (990) = port 990 (can be unblocked until 2022/02/01)

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ExplicitlyAllowedNetworkPorts
- GP name: Explicitly allowed network ports
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\ExplicitlyAllowedNetworkPorts
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ExplicitlyAllowedNetworkPorts\1 = "10080"
```

Mac information and settings

- Preference Key Name: ExplicitlyAllowedNetworkPorts
- Example value:

```
<array>
  <string>10080</string>
</array>
```

Back to top

ExternalProtocolDialogShowAlwaysOpenCheckbox

Show an "Always open" checkbox in external protocol dialog

Supported versions:

- On Windows and macOS since 79 or later

Description

This policy controls whether the "Always allow this site to open links of this type" checkbox is shown on external protocol launch confirmation prompts. This policy only applies to https:// links.

If you enable this policy, when an external protocol confirmation prompt is shown, the user can select "Always allow" to skip all future confirmation prompts for the protocol on this site.

If you disable this policy, the "Always allow" checkbox isn't displayed. The user will be prompted for confirmation every time an external protocol is invoked.

Prior to Microsoft Edge 83, if you don't configure this policy, the "Always allow" checkbox isn't displayed. The user will be prompted for confirmation every time an external protocol is invoked.

On Microsoft Edge 83, if you don't configure this policy, the checkbox visibility is controlled by the "Enable remembering protocol launch prompting preferences" flag in edge://flags

As of Microsoft Edge 84, if you don't configure this policy, when an external protocol confirmation prompt is shown, the user can select "Always allow" to skip all future confirmation prompts for the protocol on this site.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ExternalProtocolDialogShowAlwaysOpenCheckbox
- GP name: Show an "Always open" checkbox in external protocol dialog
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ExternalProtocolDialogShowAlwaysOpenCheckbox
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ExternalProtocolDialogShowAlwaysOpenCheckbox
- Example value:

```
<true/>
```

Back to top

FamilySafetySettingsEnabled

Allow users to configure Family safety and Kids Mode

Supported versions:

- On Windows and macOS since 83 or later

Description

This policy disables two family safety related features in the browser. This will hide the Family page inside Settings and navigation to edge://settings/family will be blocked. The family settings page describes what features are available with family groups with Microsoft Family Safety. Learn more about Family Safety here: (https://go.microsoft.com/fwlink/?linkid=2098432). Starting in Microsoft Edge 90, this policy also disables Kids Mode, a kid friendly browsing mode with custom themes and allow list browsing that requires the device password to exit. Learn more about Kids Mode here: (https://go.microsoft.com/fwlink/?linkid=2146910)

If you enable this policy or don't configure it, the family page in Settings will be shown and Kids Mode will be available.

If you disable this policy, the family page will not be shown, and Kids Mode will be hidden.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: FamilySafetySettingsEnabled
- GP name: Allow users to configure Family safety and Kids Mode
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: FamilySafetySettingsEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: FamilySafetySettingsEnabled
- Example value:

```
<true/>
```

Back to top

FavoritesBarEnabled

Enable favorites bar

Supported versions:

- On Windows and macOS since 77 or later

Description

Enables or disables the favorites bar.

If you enable this policy, users will see the favorites bar.

If you disable this policy, users won't see the favorites bar.

If this policy is not configured, then the user can decide to use the favorites bar or not.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: FavoritesBarEnabled
- GP name: Enable favorites bar
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: FavoritesBarEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: FavoritesBarEnabled
- Example value:

```
<true/>
```

Back to top

FetchKeepaliveDurationSecondsOnShutdown

Fetch keepalive duration on shutdown

Supported versions:

- On Windows and macOS since 90 or later

Description

Controls the duration (in seconds) that keepalive requests are allowed to prevent the browser from completing its shutdown.

If you configure this policy, the browser will block completing shutdown while it processes any outstanding keepalive requests (see https://fetch.spec.whatwg.org/#request-keepalive-flag) up to the maximum period of time specified by this policy.

If you disable or don't configure this policy, the default value of 0 seconds is used and outstanding keepalive

requests will be immediately cancelled during browser shutdown.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: FetchKeepaliveDurationSecondsOnShutdown
- GP name: Fetch keepalive duration on shutdown
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: FetchKeepaliveDurationSecondsOnShutdown
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: FetchKeepaliveDurationSecondsOnShutdown
- Example value:

```
<integer>1</integer>
```

Back to top

ForceBingSafeSearch

Enforce Bing SafeSearch

Supported versions:

- On Windows and macOS since 77 or later

Description

Ensure that queries in Bing web search are done with SafeSearch set to the value specified. Users can't change this setting.

If you configure this policy to 'BingSafeSearchNoRestrictionsMode', SafeSearch in Bing search falls back to the bing.com value.

If you configure this policy to 'BingSafeSearchModerateMode', the moderate setting is used in SafeSearch. The moderate setting filters adult videos and images but not text from search results.

If you configure this policy to 'BingSafeSearchStrictMode', the strict setting in SafeSearch is used. The strict setting filters adult text, images, and videos.

If you disable this policy or don't configure it, SafeSearch in Bing search isn't enforced, and users can set the value they want on bing.com.

Policy options mapping:

- BingSafeSearchNoRestrictionsMode (0) = Don't configure search restrictions in Bing
- BingSafeSearchModerateMode (1) = Configure moderate search restrictions in Bing
- BingSafeSearchStrictMode (2) = Configure strict search restrictions in Bing

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ForceBingSafeSearch
- GP name: Enforce Bing SafeSearch
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ForceBingSafeSearch
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: ForceBingSafeSearch
- Example value:

```
<integer>0</integer>
```

Back to top

ForceCertificatePromptsOnMultipleMatches

Configure whether Microsoft Edge should automatically select a certificate when there are multiple certificate matches for a site configured with "AutoSelectCertificateForUrls" (deprecated)

> DEPRECATED: This policy is deprecated. It is currently supported but will become obsolete in a future release.

Supported versions:

- On Windows and macOS since 81 or later

Description

This policy is deprecated because we are moving to a new policy. It won't work in Microsoft Edge version 104. The new policy to use is PromptOnMultipleMatchingCertificates.

Toggles whether users are prompted to select a certificate if there are multiple certificates available and a site is configured with AutoSelectCertificateForUrls. If you don't configure AutoSelectCertificateForUrls for a site, the user will always be prompted to select a certificate.

If you set this policy to True, Microsoft Edge will prompt a user to select a certificate for sites on the list defined in AutoSelectCertificateForUrls if and only if there is more than one certificate.

If you set this policy to False or don't configure it, Microsoft Edge will automatically select a certificate even if there are multiple matches for a certificate. The user will not be prompted to select a certificate for sites on the list defined in AutoSelectCertificateForUrls.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ForceCertificatePromptsOnMultipleMatches
- GP name: Configure whether Microsoft Edge should automatically select a certificate when there are multiple certificate matches for a site configured with "AutoSelectCertificateForUrls" (deprecated)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ForceCertificatePromptsOnMultipleMatches
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ForceCertificatePromptsOnMultipleMatches
- Example value:

```
<true/>
```

Back to top

ForceEphemeralProfiles

Enable use of ephemeral profiles

Supported versions:

- On Windows and macOS since 77 or later

Description

Controls whether user profiles are switched to ephemeral mode. An ephemeral profile is created when a session begins, is deleted when the session ends, and is associated with the user's original profile.

If you enable this policy, profiles run in ephemeral mode. This lets users work from their own devices without

saving browsing data to those devices. If you enable this policy as an OS policy (by using GPO on Windows, for example), it applies to every profile on the system.

If you disable this policy or don't configure it, users get their regular profiles when they sign in to the browser.

In ephemeral mode, profile data is saved on disk only for the length of the user session. Features like browser history, extensions and their data, web data like cookies, and web databases aren't saved after the browser is closed. This doesn't prevent a user from manually downloading any data to disk, or from saving pages or printing them. If the user has enabled sync, all data is preserved in their sync accounts just like with regular profiles. Users can also use InPrivate browsing in ephemeral mode unless you explicitly disable this.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ForceEphemeralProfiles
- GP name: Enable use of ephemeral profiles
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ForceEphemeralProfiles
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ForceEphemeralProfiles
- Example value:

```
<true/>
```

Back to top

ForceGoogleSafeSearch

Enforce Google SafeSearch

Supported versions:

- On Windows and macOS since 77 or later

Description

Forces queries in Google Web Search to be performed with SafeSearch set to active, and prevents users from changing this setting.

If you enable this policy, SafeSearch in Google Search is always active.

If you disable this policy or don't configure it, SafeSearch in Google Search isn't enforced.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ForceGoogleSafeSearch
- GP name: Enforce Google SafeSearch
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ForceGoogleSafeSearch
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: ForceGoogleSafeSearch
- Example value:

```
<false/>
```

Back to top

ForceLegacyDefaultReferrerPolicy

Use a default referrer policy of no-referrer-when-downgrade (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 88.

Supported versions:

- On Windows and macOS since 81, until 88

Description

This policy doesn't work because it was only intended to be a short-term mechanism to give enterprises more time to update their web content if it was found to be incompatible with the new default referrer policy.

Microsoft Edge's default referrer policy was strengthened from the value of no-referrer-when-downgrade to the more secure strict-origin-when-cross-origin.

When this enterprise policy is enabled, Microsoft Edge's default referrer policy will be set to its old value of no-referrer-when-downgrade.

This enterprise policy is disabled by default.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ForceLegacyDefaultReferrerPolicy
- GP name: Use a default referrer policy of no-referrer-when-downgrade (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ForceLegacyDefaultReferrerPolicy
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: ForceLegacyDefaultReferrerPolicy
- Example value:

```
<false/>
```

Back to top

ForceMajorVersionToMinorPositionInUserAgent

Enable or disable freezing the User-Agent string at major version 99

Supported versions:

- On Windows and macOS since 99 or later

Description

This policy controls whether the User-Agent string major version should be frozen at 99.

The User-Agent request header lets websites identify the application, operating system, vendor, and/or version of the requesting user agent. Some websites make assumptions about how this header is formatted and may encounter issues with version strings that include three digits in the major position (for example, 100.0.0.0).

Setting the policy to 'Default' or leaving it unset will default to browser settings for the User-Agent string major version. If set to 'ForceEnabled', the User-Agent string will always report the major version as 99 and include the browser's major version in the minor position. For example, browser version 101.0.0.0 would send a User-Agent request header that reports version 99.101.0.0. If set to 'ForceDisabled', the User-Agent string will not freeze the major version.

This policy is temporary and will be deprecated in the future. Note that if this policy and User-Agent Reduction are both enabled, the User-Agent version string will always be 99.0.0.0.

Policy options mapping:

- Default (0) = Default to browser settings for User-Agent string version.
- ForceDisabled (1) = The User-Agent string will not freeze the major version.
- ForceEnabled (2) = The User-Agent string will freeze the major version as 99 and include the browser's major version in the minor position.

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ForceMajorVersionToMinorPositionInUserAgent
- GP name: Enable or disable freezing the User-Agent string at major version 99
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ForceMajorVersionToMinorPositionInUserAgent
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: ForceMajorVersionToMinorPositionInUserAgent
- Example value:

```
<integer>0</integer>
```

Back to top

ForceNetworkInProcess

Force networking code to run in the browser process (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 83.

Supported versions:

- On Windows since 78, until 83

Description

This policy doesn't work because it was only intended to be a short-term mechanism to give enterprises more time to migrate to 3rd party software that doesn't depend on hooking networking APIs. Proxy servers are recommended over LSPs and Win32 API patching.

This policy forces networking code to run in the browser process.

This policy is disabled by default. If enabled, users are open to security issues when the networking process is sandboxed.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ForceNetworkInProcess
- GP name: Force networking code to run in the browser process (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ForceNetworkInProcess
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

ForceSync

Force synchronization of browser data and do not show the sync consent prompt

Supported versions:

- On Windows and macOS since 86 or later

Description

Forces data synchronization in Microsoft Edge. This policy also prevents the user from turning sync off.

If you don't configure this policy, users will be able to turn sync on or off. If you enable this policy, users will not be able to turn sync off.

For this policy to work as intended, BrowserSignin policy must not be configured, or must be set to enabled. If BrowserSignin is set to disabled, then ForceSync will not take affect.

SyncDisabled must not be configured or must be set to False. If this is set to True, ForceSync will not take affect. If you wish to ensure specific datatypes sync or do not sync, use the ForceSyncTypes policy and SyncTypesListDisabled policy.

0 = Do not automatically start sync and show the sync consent (default) 1 = Force sync to be turned on for Azure AD/Azure AD-Degraded user profile and do not show the sync consent prompt

Supported features:

- Can be mandatory: Yes
- Can be recommended: No

- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ForceSync
- GP name: Force synchronization of browser data and do not show the sync consent prompt
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ForceSync
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ForceSync
- Example value:

```
<true/>
```

Back to top

ForceSyncTypes

Configure the list of types that are included for synchronization

Supported versions:

- On Windows and macOS since 96 or later

Description

If you enable this policy all the specified data types will be included for synchronization for Azure AD/Azure AD-Degraded user profiles. This policy can be used to ensure the type of data uploaded to the Microsoft Edge synchronization service.

You can provide one of the following data types for this policy: "favorites", "settings", "passwords", "addressesAndMore", "extensions", "history", "openTabs", and "collections". The "apps" data type will be supported starting in Microsoft Edge version 100. Note that these data type names are case sensitive.

Users will not be able to override the enabled data types.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ForceSyncTypes
- GP name: Configure the list of types that are included for synchronization
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\ForceSyncTypes
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ForceSyncTypes\1 = "favorites"
```

Mac information and settings

- Preference Key Name: ForceSyncTypes
- Example value:

```
<array>
  <string>favorites</string>
</array>
```

Back to top

ForceYouTubeRestrict

Force minimum YouTube Restricted Mode

Supported versions:

- On Windows and macOS since 77 or later

Description

Enforces a minimum Restricted Mode on YouTube and prevents users from picking a less restricted mode.

Set to 'Strict' to enforce Strict Restricted Mode on YouTube.

Set to 'Moderate' to enforce the user to only use Moderate Restricted Mode and Strict Restricted Mode on YouTube. They can't disable Restricted Mode.

Set to 'Off' or don't configure this policy to not enforce Restricted Mode on YouTube. External policies such as YouTube policies might still enforce Restricted Mode.

Policy options mapping:

- Off (0) = Do not enforce Restricted Mode on YouTube
- Moderate (1) = Enforce at least Moderate Restricted Mode on YouTube
- Strict (2) = Enforce Strict Restricted Mode for YouTube

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ForceYouTubeRestrict
- GP name: Force minimum YouTube Restricted Mode
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ForceYouTubeRestrict
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: ForceYouTubeRestrict
- Example value:

```
<integer>0</integer>
```

Back to top

FullscreenAllowed

Allow full screen mode

Supported versions:

- On Windows since 77 or later

Description

Set the availability of full screen mode - all Microsoft Edge UI is hidden and only web content is visible.

If you enable this policy or don't configure it, the user, apps, and extensions with appropriate permissions can enter full screen mode.

If you disable this policy, users, apps, and extensions can't enter full screen mode.

Opening Microsoft Edge in kiosk mode using the command line is unavailable when full screen mode is disabled.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: FullscreenAllowed
- GP name: Allow full screen mode

- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: FullscreenAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

GloballyScopeHTTPAuthCacheEnabled

Enable globally scoped HTTP auth cache

Supported versions:

- On Windows and macOS since 81 or later

Description

This policy configures a single global per profile cache with HTTP server authentication credentials.

If you disable or don't set this policy, the browser will use the default behavior of cross-site auth, which as of version 80, will be to scope HTTP server authentication credentials by top-level site. So, if two sites use resources from the same authenticating domain, credentials will need to be provided independently in the context of both sites. Cached proxy credentials will be reused across sites.

If you enable this policy HTTP auth credentials entered in the context of one site will automatically be used in the context of another site.

Enabling this policy leaves sites open to some types of cross-site attacks, and allows users to be tracked across sites even without cookies by adding entries to the HTTP auth cache using credentials embedded in URLs.

This policy is intended to give enterprises depending on the legacy behavior a chance to update their login procedures and will be removed in the future.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: GloballyScopeHTTPAuthCacheEnabled
- GP name: Enable globally scoped HTTP auth cache
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A

- Value Name: GloballyScopeHTTPAuthCacheEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: GloballyScopeHTTPAuthCacheEnabled
- Example value:

```
<false/>
```

Back to top

GoToIntranetSiteForSingleWordEntryInAddressBar

Force direct intranet site navigation instead of searching on single word entries in the Address Bar

Supported versions:

- On Windows and macOS since 78 or later

Description

If you enable this policy, the top auto-suggest result in the address bar suggestion list will navigate to intranet sites if the text entered in the address bar is a single word without punctuation.

Default navigation when typing a single word without punctuation will conduct a navigation to an intranet site matching the entered text.

If you enable this policy, the second auto-suggest result in the address bar suggestion list will conduct a web search exactly as it was entered, provided that this text is a single word without punctuation. The default search provider will be used unless a policy to prevent web search is also enabled.

Two effects of enabling this policy are:

Navigation to sites in response to single word queries that would typically resolve to a history item will no longer happen. Instead, the browser will attempt navigate to internal sites that may not exist in an organization's intranet. This will result in a 404 error.

Popular, single-word search terms will require manual selection of search suggestions to properly conduct a search.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: GoToIntranetSiteForSingleWordEntryInAddressBar
- GP name: Force direct intranet site navigation instead of searching on single word entries in the Address Bar
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: GoToIntranetSiteForSingleWordEntryInAddressBar
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: GoToIntranetSiteForSingleWordEntryInAddressBar
- Example value:

```
<false/>
```

Back to top

HSTSPolicyBypassList

Configure the list of names that will bypass the HSTS policy check

Supported versions:

- On Windows and macOS since 79 or later

Description

Setting the policy specifies a list of hostnames that bypass preloaded HSTS upgrades from http to https.

Only single-label hostnames are allowed in this policy, and this policy only applies to static HSTS-preloaded entries (for example, "app", "new", "search", "play"). This policy does not prevent HSTS upgrades for servers that have dynamically requested HSTS upgrades using a Strict-Transport-Security response header.

Supplied hostnames must be canonicalized: Any IDNs must be converted to their A-label format, and all ASCII letters must be lowercase. This policy only applies to the specific single-label hostnames specified, not to subdomains of those names.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: HSTSPolicyBypassList
- GP name: Configure the list of names that will bypass the HSTS policy check
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\HSTSPolicyBypassList
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\HSTSPolicyBypassList\1 = "meet"
```

Mac information and settings

- Preference Key Name: HSTSPolicyBypassList
- Example value:

```
<array>
  <string>meet</string>
</array>
```

Back to top

HardwareAccelerationModeEnabled

Use hardware acceleration when available

Supported versions:

- On Windows and macOS since 77 or later

Description

Specifies whether to use hardware acceleration if it's available. If you enable this policy or don't configure it, hardware acceleration is enabled unless a GPU feature is explicitly blocked.

If you disable this policy, hardware acceleration is disabled.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: HardwareAccelerationModeEnabled
- GP name: Use hardware acceleration when available
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: HardwareAccelerationModeEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: HardwareAccelerationModeEnabled
- Example value:

```
<true/>
```

Back to top

HeadlessModeEnabled

Control use of the Headless Mode

Supported versions:

- On Windows and macOS since 92 or later

Description

This policy setting lets you decide whether users can launch Microsoft Edge in headless mode.

If you enable or don't configure this policy, Microsoft Edge allows use of the headless mode.

If you disable this policy, Microsoft Edge denies use of the headless mode.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: HeadlessModeEnabled
- GP name: Control use of the Headless Mode
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: HeadlessModeEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: HeadlessModeEnabled
- Example value:

```
<true/>
```

Back to top

HideFirstRunExperience

Hide the First-run experience and splash screen

Supported versions:

- On Windows and macOS since 80 or later

Description

If you enable this policy, the First-run experience and the splash screen will not be shown to users when they run Microsoft Edge for the first time.

For the configuration options shown in the First Run Experience, the browser will default to the following:

-On the New Tab Page, the feed type will be set to MSN News and the layout to Inspirational.

-The user will still be automatically signed into Microsoft Edge if the Windows account is of Azure AD or MSA type.

-Sync will not be enabled by default and users will be prompted to choose whether they'd like to sync on browser startup. You can use the ForceSync or the SyncDisabled policy to configure sync and the sync consent prompt.

If you disable or don't configure this policy, the First-run experience and the Splash screen will be shown.

Note: The specific configuration options shown to the user in the First Run Experience, can also be managed by using other specific policies. You can use the HideFirstRunExperience policy in combination with these policies to configure a specific browser experience on your managed devices. Some of these other policies are:

-AutoImportAtFirstRun

-NewTabPageLocation

-NewTabPageSetFeedType

-ForceSync

-SyncDisabled

-BrowserSignin

-NonRemovableProfileEnabled

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: HideFirstRunExperience
- GP name: Hide the First-run experience and splash screen
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: HideFirstRunExperience
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: HideFirstRunExperience
- Example value:

```
<true/>
```

Back to top

HideInternetExplorerRedirectUXForIncompatibleSitesEnabled

Hide the one-time redirection dialog and the banner on Microsoft Edge

Supported versions:

- On Windows since 87 or later

Description

This policy gives an option to disable one-time redirection dialog and the banner. When this policy is enabled, users will not see both the one-time dialog and the banner. Users will continue to be redirected to Microsoft Edge when they encounter an incompatible website on Internet Explorer, but their browsing data will not be imported.

- If you enable this policy the one-time redirection dialog and banner will never be shown to users. Users' browsing data will not be imported when a redirection happens.
- If you disable or don't set this policy, the redirection dialog will be shown on the first redirection and the persistent redirection banner will be shown to users on sessions that begin with a redirection. Users' browsing data will be imported every time user encounters such redirection (ONLY IF user consents to it on the one-time dialog).

  Supported features:

  - Can be mandatory: Yes
  - Can be recommended: No
  - Dynamic Policy Refresh: No - Requires browser restart

  Data Type:

  - Boolean

  Windows information and settings

  Group Policy (ADMX) info

  - GP unique name: HideInternetExplorerRedirectUXForIncompatibleSitesEnabled
  - GP name: Hide the one-time redirection dialog and the banner on Microsoft Edge
  - GP path (Mandatory): Administrative Templates/Microsoft Edge/
  - GP path (Recommended): N/A
  - GP ADMX file name: MSEdge.admx

  Windows Registry Settings

  - Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
  - Path (Recommended): N/A
  - Value Name: HideInternetExplorerRedirectUXForIncompatibleSitesEnabled
  - Value Type: REG_DWORD

  Example value:

```
0x00000001
```

Back to top

HideRestoreDialogEnabled

Hide restore pages dialog after browser crash

Supported versions:

- On Windows and macOS since 100 or later

Description

This policy gives an option to hide the "Restore pages" dialog after Microsoft Edge has crashed. The "Restore pages" dialog gives users the option to restore the pages that were previously open before Microsoft Edge crashed.

If you enable this policy, the "Restore pages" dialog will not be shown. In the event of a crash, Microsoft Edge will not restore previous tabs and will start the session with a new tab page.

If you disable or don't set this policy, the "Restore pages" dialog will be shown.

If you set this policy, do not set the ClearBrowsingDataOnExit or SavingBrowserHistoryDisabled policy since that prevents history from being saved which also disables the dialog.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: HideRestoreDialogEnabled
- GP name: Hide restore pages dialog after browser crash
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: HideRestoreDialogEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: HideRestoreDialogEnabled
- Example value:

```
<false/>
```

Back to top

HubsSidebarEnabled

Show Hubs Sidebar

Supported versions:

- On Windows and macOS since 99 or later

Description

Sidebar is a launcher bar on the right side of Microsoft Edge's screen.

If you enable or don't configure this policy, the Sidebar will be shown. If you disable this policy, the Sidebar will never be shown.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: HubsSidebarEnabled
- GP name: Show Hubs Sidebar
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: HubsSidebarEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: HubsSidebarEnabled
- Example value:

```
<true/>
```

Back to top

ImportAutofillFormData

Allow importing of autofill form data

Supported versions:

- On Windows and macOS since 77 or later

Description

Allows users to import autofill form data from another browser into Microsoft Edge.

If you enable this policy, the option to manually import autofill data is automatically selected.

If you disable this policy, autofill form data isn't imported at first run, and users can't import it manually.

If you don't configure this policy, autofill data is imported at first run, and users can choose whether to import this data manually during later browsing sessions.

You can set this policy as a recommendation. This means that Microsoft Edge will import autofill data on first run, but users can select or clear **autofill data** option during manual import.

Note: This policy currently manages importing from Google Chrome (on Windows 7, 8, and 10 and on macOS) and Mozilla Firefox (on Windows 7, 8, and 10 and on macOS) browsers.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ImportAutofillFormData
- GP name: Allow importing of autofill form data
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ImportAutofillFormData
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ImportAutofillFormData
- Example value:

```
<true/>
```

Back to top

ImportBrowserSettings

Allow importing of browser settings

Supported versions:

- On Windows and macOS since 78 or later

Description

Allows users to import browser settings from another browser into Microsoft Edge.

If you enable this policy, the **Browser settings** check box is automatically selected in the **Import browser data** dialog box.

If you disable this policy, browser settings aren't imported at first run, and users can't import them manually.

If you don't configure this policy, browser settings are imported at first run, and users can choose whether to import them manually during later browsing sessions.

You can also set this policy as a recommendation. This means that Microsoft Edge imports the settings on first run, but users can select or clear the **browser settings** option during manual import.

Note: This policy currently manages importing Google Chrome (on Windows 7, 8, and 10 and on macOS).

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ImportBrowserSettings
- GP name: Allow importing of browser settings
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ImportBrowserSettings
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ImportBrowserSettings
- Example value:

```
<true/>
```

Back to top

ImportCookies

Allow importing of Cookies

Supported versions:

- On Windows and macOS since 81 or later

Description

Allows users to import Cookies from another browser into Microsoft Edge.

If you disable this policy, Cookies aren't imported on first run.

If you don't configure this policy, Cookies are imported on first run.

You can also set this policy as a recommendation. This means that Microsoft Edge imports Cookies on first run.

Note: This policy currently manages importing Google Chrome (on Windows 7, 8, and 10 and on macOS).

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ImportCookies
- GP name: Allow importing of Cookies
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ImportCookies
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ImportCookies
- Example value:

```
<true/>
```

Back to top

ImportExtensions

Allow importing of extensions

Supported versions:

- On Windows and macOS since 81 or later

Description

Allows users to import extensions from another browser into Microsoft Edge.

If you enable this policy, the **Extensions** check box is automatically selected in the **Import browser data** dialog box.

If you disable this policy, extensions aren't imported at first run, and users can't import them manually.

If you don't configure this policy, extensions are imported at first run, and users can choose whether to import them manually during later browsing sessions.

You can also set this policy as a recommendation. This means that Microsoft Edge imports extensions on first run, but users can select or clear the **extensions** option during manual import.

Note: This policy currently only supports importing from Google Chrome (on Windows 7, 8, and 10 and on macOS).

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ImportExtensions
- GP name: Allow importing of extensions
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ImportExtensions
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ImportExtensions
- Example value:

```
<true/>
```

Back to top

ImportFavorites

Allow importing of favorites

Supported versions:

- On Windows and macOS since 77 or later

Description

Allows users to import favorites from another browser into Microsoft Edge.

If you enable this policy, the **Favorites** check box is automatically selected in the **Import browser data** dialog box.

If you disable this policy, favorites aren't imported at first run, and users can't import them manually.

If you don't configure this policy, favorites are imported at first run, and users can choose whether to import them manually during later browsing sessions.

You can also set this policy as a recommendation. This means that Microsoft Edge imports favorites on first run, but users can select or clear the **favorites** option during manual import.

Note: This policy currently manages importing from Internet Explorer (on Windows 7, 8, and 10), Google Chrome (on Windows 7, 8, and 10 and on macOS), Mozilla Firefox (on Windows 7, 8, and 10 and on macOS), and Apple Safari (on macOS) browsers.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ImportFavorites
- GP name: Allow importing of favorites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ImportFavorites
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ImportFavorites
- Example value:

```
<true/>
```

Back to top

ImportHistory

Allow importing of browsing history

Supported versions:

- On Windows and macOS since 77 or later

Description

Allows users to import their browsing history from another browser into Microsoft Edge.

If you enable this policy, the **Browsing history** check box is automatically selected in the **Import browser data** dialog box.

If you disable this policy, browsing history data isn't imported at first run, and users can't import this data manually.

If you don't configure this policy, browsing history data is imported at first run, and users can choose whether to import it manually during later browsing sessions.

You can also set this policy as a recommendation. This means that Microsoft Edge imports browsing history on first run, but users can select or clear the **history** option during manual import.

Note: This policy currently manages importing from Internet Explorer (on Windows 7, 8, and 10), Google Chrome (on Windows 7, 8, and 10 and on macOS), Mozilla Firefox (on Windows 7, 8, and 10 and on macOS), and Apple Safari (macOS) browsers.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ImportHistory
- GP name: Allow importing of browsing history
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ImportHistory
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ImportHistory
- Example value:

```
<true/>
```

Back to top

ImportHomepage

Allow importing of home page settings

Supported versions:

- On Windows and macOS since 77 or later

Description

Allows users to import their home page setting from another browser into Microsoft Edge.

If you enable this policy, the option to manually import the home page setting is automatically selected.

If you disable this policy, the home page setting isn't imported at first run, and users can't import it manually.

If you don't configure this policy, the home page setting is imported at first run, and users can choose whether to import this data manually during later browsing sessions.

You can set this policy as a recommendation. This means that Microsoft Edge imports the home page setting on first run, but users can select or clear the **home page** option during manual import.

Note: This policy currently manages importing from Internet Explorer (on Windows 7, 8, and 10).

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ImportHomepage
- GP name: Allow importing of home page settings
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ImportHomepage
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ImportHomepage
- Example value:

```
<true/>
```

Back to top

ImportOnEachLaunch

Allow import of data from other browsers on each Microsoft Edge launch

Supported versions:

- On Windows since 104 or later

Description

If you enable this policy, users will see a prompt to import their browsing data from other browsers on each Microsoft Edge launch.

If you disable this policy, users will never see a prompt to import their browsing data from other browsers on each Microsoft Edge launch.

If the policy is left unconfigured, users can activate this feature from a Microsoft Edge prompt or from the Settings page.

Note: A similar policy named AutoImportAtFirstRun exists. This policy should be used if you want to import supported data from other browsers only once while setting up your device.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ImportOnEachLaunch
- GP name: Allow import of data from other browsers on each Microsoft Edge launch
- GP path (Mandatory): Administrative Templates/Microsoft Edge/

- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ImportOnEachLaunch
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

ImportOpenTabs

Allow importing of open tabs

Supported versions:

- On Windows and macOS since 79 or later

Description

Allows users to import open and pinned tabs from another browser into Microsoft Edge.

If you enable this policy, the **Open tabs** check box is automatically selected in the **Import browser data** dialog box.

If you disable this policy, open tabs aren't imported at first run, and users can't import them manually.

If you don't configure this policy, open tabs are imported at first run, and users can choose whether to import them manually during later browsing sessions.

You can also set this policy as a recommendation. This means that Microsoft Edge imports open tabs on first run, but users can select or clear the **Open tabs** option during manual import.

Note: This policy currently only supports importing from Google Chrome (on Windows 7, 8, and 10 and on macOS).

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ImportOpenTabs
- GP name: Allow importing of open tabs
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ImportOpenTabs

- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ImportOpenTabs
- Example value:

```
<true/>
```

Back to top

ImportPaymentInfo

Allow importing of payment info

Supported versions:

- On Windows and macOS since 77 or later

Description

Allows users to import payment info from another browser into Microsoft Edge.

If you enable this policy, the **payment info** check box is automatically selected in the **Import browser data** dialog box.

If you disable this policy, payment info isn't imported at first run, and users can't import it manually.

If you don't configure this policy, payment info is imported at first run, and users can choose whether to import it manually during later browsing sessions.

You can also set this policy as a recommendation. This means that Microsoft Edge imports payment info on first run, but users can select or clear the **payment info** option during manual import.

Note: This policy currently manages importing from Google Chrome (on Windows 7, 8, and 10 and on macOS).

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ImportPaymentInfo
- GP name: Allow importing of payment info
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ImportPaymentInfo
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ImportPaymentInfo
- Example value:

```
<true/>
```

Back to top

ImportSavedPasswords

Allow importing of saved passwords

Supported versions:

- On Windows and macOS since 77 or later

Description

Allows users to import saved passwords from another browser into Microsoft Edge.

If you enable this policy, the option to manually import saved passwords is automatically selected.

If you disable this policy, saved passwords aren't imported on first run, and users can't import them manually.

If you don't configure this policy, passwords are imported at first run, and users can choose whether to import them manually during later browsing sessions.

You can set this policy as a recommendation. This means that Microsoft Edge imports passwords on first run, but users can select or clear the **passwords** option during manual import.

Note: This policy currently manages importing from Internet Explorer (on Windows 7, 8, and 10), Google Chrome (on Windows 7, 8, and 10 and on macOS), and Mozilla Firefox (on Windows 7, 8, and 10 and on macOS) browsers.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ImportSavedPasswords
- GP name: Allow importing of saved passwords
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ImportSavedPasswords
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ImportSavedPasswords
- Example value:

```
<true/>
```

Back to top

ImportSearchEngine

Allow importing of search engine settings

Supported versions:

- On Windows and macOS since 77 or later

Description

Allows users to import search engine settings from another browser into Microsoft Edge.

If you enable, this policy, the option to import search engine settings is automatically selected.

If you disable this policy, search engine settings aren't imported at first run, and users can't import them manually.

If you don't configure this policy, search engine settings are imported at first run, and users can choose whether to import this data manually during later browsing sessions.

You can set this policy as a recommendation. This means that Microsoft Edge imports search engine settings on first run, but users can select or clear the **search engine** option during manual import.

Note: This policy currently manages importing from Internet Explorer (on Windows 7, 8, and 10).

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ImportSearchEngine
- GP name: Allow importing of search engine settings
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ImportSearchEngine
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ImportSearchEngine
- Example value:

```
<true/>
```

Back to top

ImportShortcuts

Allow importing of shortcuts

Supported versions:

- On Windows and macOS since 81 or later

Description

Allows users to import Shortcuts from another browser into Microsoft Edge.

If you disable this policy, Shortcuts aren't imported on first run.

If you don't configure this policy, Shortcuts are imported on first run.

You can also set this policy as a recommendation. This means that Microsoft Edge imports Shortcuts on first run.

Note: This policy currently manages importing from Google Chrome (on Windows 7, 8, and 10 and on macOS).

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ImportShortcuts
- GP name: Allow importing of shortcuts
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ImportShortcuts
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ImportShortcuts
- Example value:

```
<true/>
```

Back to top

ImportStartupPageSettings

Allow importing of startup page settings

Supported versions:

- On Windows since 91 or later

Description

Allows users to import Startup settings from another browser into Microsoft Edge.

If you enable this policy, the Startup settings are always imported.

If you disable this policy, startup settings are not imported at first run or at manual import.

If you don't configure this policy, startup settings are imported at first run, and users can choose whether to import this data manually by selecting browser settings option during later browsing sessions.

You can set this policy as a recommendation. This means that Microsoft Edge will import startup settings on first run, but users can select or clear **browser settings** option during manual import.

Note: This policy currently manages importing from Microsoft Edge Legacy and Google Chrome (on Windows 7, 8, and 10) browsers.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ImportStartupPageSettings
- GP name: Allow importing of startup page settings
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ImportStartupPageSettings
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

InAppSupportEnabled

In-app support Enabled

Supported versions:

- On Windows and macOS since 98 or later

Description

Microsoft Edge uses the in-app support feature (enabled by default) to allow users to contact our support agents directly from the browser. Also, by default, users can't disable (turn off) the in-app support feature.

If you enable this policy or don't configure it, users can invoke in-app support.

If you disable this policy, users can't invoke in-app support.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InAppSupportEnabled
- GP name: In-app support Enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InAppSupportEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: InAppSupportEnabled
- Example value:

```
<true/>
```

Back to top

InPrivateModeAvailability

Configure InPrivate mode availability

Supported versions:

- On Windows and macOS since 77 or later

Description

Specifies whether the user can open pages in InPrivate mode in Microsoft Edge.

If you don't configure this policy or set it to 'Enabled', users can open pages in InPrivate mode.

Set this policy to 'Disabled' to stop users from using InPrivate mode.

Set this policy to 'Forced' to always use InPrivate mode.

Policy options mapping:

- Enabled (0) = InPrivate mode available
- Disabled (1) = InPrivate mode disabled
- Forced (2) = InPrivate mode forced

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InPrivateModeAvailability
- GP name: Configure InPrivate mode availability
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InPrivateModeAvailability
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: InPrivateModeAvailability
- Example value:

```
<integer>1</integer>
```

Back to top

InsecureFormsWarningsEnabled

Enable warnings for insecure forms

Supported versions:

- On Windows and macOS since 86 or later

Description

This policy controls the handling of insecure forms (forms submitted over HTTP) embedded in secure (HTTPS) sites in the browser. If you enable this policy or don't set it, a full page warning will be shown when an insecure form is submitted. Additionally, a warning bubble will be shown next to the form fields when they are focused, and autofill will be disabled for those forms. If you disable this policy, warnings will not be shown for insecure forms, and autofill will work normally.

Supported features:

- Can be mandatory: Yes

- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InsecureFormsWarningsEnabled
- GP name: Enable warnings for insecure forms
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InsecureFormsWarningsEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: InsecureFormsWarningsEnabled
- Example value:

```
<true/>
```

Back to top

IntensiveWakeUpThrottlingEnabled

Control the IntensiveWakeUpThrottling feature

Supported versions:

- On Windows and macOS since 85 or later

Description

When enabled the IntensiveWakeUpThrottling feature causes Javascript timers in background tabs to be aggressively throttled and coalesced, running no more than once per minute after a page has been backgrounded for 5 minutes or more.

This is a web standards compliant feature, but it may break functionality on some websites by causing certain actions to be delayed by up to a minute. However, it results in significant CPU and battery savings when enabled. See https://bit.ly/30b1XR4 for more details.

If you enable this policy, the feature will be force enabled, and users will not be able to override this setting. If you disable this policy, the feature will be force disabled, and users will not be able to override this setting. If you don't configure this policy, the feature will be controlled by its own internal logic. Users can manually configure this setting.

Note that the policy is applied per renderer process, with the most recent value of the policy setting in force when a renderer process starts. A full restart is required to ensure that all the loaded tabs receive a consistent policy setting. It is harmless for processes to be running with different values of this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: IntensiveWakeUpThrottlingEnabled
- GP name: Control the IntensiveWakeUpThrottling feature
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: IntensiveWakeUpThrottlingEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: IntensiveWakeUpThrottlingEnabled
- Example value:

```
<true/>
```

Back to top

InternetExplorerIntegrationAlwaysUseOSCapture

Always use the OS capture engine to avoid issues with capturing Internet Explorer mode tabs

Supported versions:

- On Windows since 106 or later

Description

Configure this policy to control whether Microsoft Edge will use the "OS capture engine" or the "Browser capture engine" when capturing browser windows in the same process using the screen-share APIs.

You should configure this policy if you want to capture the contents of Internet Explorer mode tabs. However, enabling this policy may negatively impact performance when capturing browser windows in the same process.

This policy only affects window capture, not tab capture. The contents of Internet Explorer mode tabs will not be captured when you choose to capture only a single tab, even if you configure this policy.

If you enable this policy, Microsoft Edge will always use the OS capture engine for window capture. Internet Explorer mode tabs will have their contents captured.

If you disable or don't configure this policy, Microsoft Edge will use the Browser capture engine for browser windows in the same process. Internet Explorer mode tabs in these windows will not have their contents captured.

To learn more about Internet Explorer mode, see https://go.microsoft.com/fwlink/?linkid=2174004

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationAlwaysUseOSCapture
- GP name: Always use the OS capture engine to avoid issues with capturing Internet Explorer mode tabs
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerIntegrationAlwaysUseOSCapture
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

InternetExplorerIntegrationAlwaysWaitForUnload

Wait for Internet Explorer mode tabs to completely unload before ending the browser session

Supported versions:

- On Windows since 105 or later

Description

This policy causes Microsoft Edge to continue running until all Internet Explorer tabs have completely finished unloading. This allows Internet Explorer plugins like ActiveX controls to perform additional critical work even after the browser has been closed. However, this can cause stability and performance issues, and Microsoft Edge processes may remain active in the background with no visible windows if the webpage or plugin prevents Internet Explorer from unloading. This policy should only be used if your organization depends on a plugin that requires this behavior.

If you enable this policy, Microsoft Edge will always wait for Internet Explorer mode tabs to fully unload before ending the browser session.

If you disable or don't configure this policy, Microsoft Edge will not always wait for Internet Explorer mode tabs to fully unload before ending the browser session.

To learn more about Internet Explorer mode, see https://go.microsoft.com/fwlink/?linkid=2174004

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationAlwaysWaitForUnload
- GP name: Wait for Internet Explorer mode tabs to completely unload before ending the browser session
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerIntegrationAlwaysWaitForUnload
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

InternetExplorerIntegrationCloudNeutralSitesReporting

Configure reporting of potentially misconfigured neutral site URLs to the M365 Admin Center Site Lists app

Supported versions:

- On Windows since 99 or later

Description

This setting lets you enable reporting of sites that might need to be configured as a neutral site on the Enterprise Mode Site List. The user must be signed into Microsoft Edge with a valid work or school account for reports to be sent, and the user's account tenant must match the tenant specified by the policy.

If you configure this policy, Microsoft Edge will send a report to the M365 Admin Center Site Lists app when a navigation appears stuck redirecting back and forth between the Microsoft Edge and Internet Explorer engines several times. This usually indicates that redirection to an authentication server is switching engines, which repeatedly fails in a loop. The report will show the URL of the site that is the redirect target, minus any query string or fragment. The user's identity isn't reported.

For this reporting to work correctly, you must have successfully visited the Microsoft Edge Site Lists app in the M365 Admin Center at least once. This activates a per-tenant storage account used to store these reports. Microsoft Edge will still attempt to send reports if this step hasn't been completed. However, the reports will not be stored in the Site Lists app.

When enabling this policy, you must specify your O365 tenant ID. To learn more about finding your O365 tenant ID, see https://go.microsoft.com/fwlink/?linkid=2185668

If you disable or don't configure this policy, Microsoft Edge will never send reports about potentially misconfigured neutral sites to the Site Lists app.

To learn more about Internet Explorer mode, see https://go.microsoft.com/fwlink/?linkid=2165707

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationCloudNeutralSitesReporting
- GP name: Configure reporting of potentially misconfigured neutral site URLs to the M365 Admin Center Site Lists app
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerIntegrationCloudNeutralSitesReporting
- Value Type: REG_SZ

Example value:

```
"aba95e58-070f-4784-8dcd-e5fd46c2c6d6"
```

Back to top

InternetExplorerIntegrationCloudSiteList

Configure the Enterprise Mode Cloud Site List

Supported versions:

- On Windows since 93 or later

Description

The Microsoft Edge Site Lists setting in the M365 Admin Center allows you to host your site list(s) in a compliant cloud location and manage the contents of your site list(s) through the built-in experience. This setting allows you to specify which site list within the M365 Admin Center to deploy to your users. The user must be signed into Microsoft Edge with a valid work or school account. Otherwise, Microsoft Edge will not download the site list from the cloud location.

This setting is applicable only when the InternetExplorerIntegrationLevel setting is configured.

If you configure this policy, Microsoft Edge will use the specified site list. When enabled, you can enter the identifier of the site list that you created and published to the cloud in M365 Admin Center.

This setting takes precedence over Microsoft Edge's InternetExplorerIntegrationSiteList policy as well as Internet Explorer's site list setting (Use the Enterprise mode IE website list). If you disable or don't configure this policy, Microsoft Edge will use the InternetExplorerIntegrationSiteList policy instead.

To learn more about Internet Explorer mode, see https://go.microsoft.com/fwlink/?linkid=2165707

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationCloudSiteList
- GP name: Configure the Enterprise Mode Cloud Site List
- GP path (Mandatory): Administrative Templates/Microsoft Edge/

- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerIntegrationCloudSiteList
- Value Type: REG_SZ

Example value:

```
"aba95e58-070f-4784-8dcd-e5fd46c2c6d6"
```

Back to top

InternetExplorerIntegrationCloudUserSitesReporting

Configure reporting of IE Mode user list entries to the M365 Admin Center Site Lists app

Supported versions:

- On Windows since 99 or later

Description

This setting lets you enable reporting of sites that Microsoft Edge users add to their local IE Mode site list. The user must be signed into Microsoft Edge with a valid work or school account for reports to be sent, and the user's account tenant must match the tenant specified by the policy.

If you configure this policy, Microsoft Edge will send a report to the M365 Admin Center Site Lists app when a user adds a site to their local IE mode site list. The report will show the URL of the site the user added, minus any query string or fragment. The user's identity isn't reported.

For this reporting to work correctly, you must have successfully visited the Microsoft Edge Site Lists app in the M365 Admin Center at least once. This activates a per-tenant storage account used to store these reports. Microsoft Edge will still attempt to send reports if this step hasn't been completed. However, the reports will not be stored in the Site Lists app.

When enabling this policy, you must specify your O365 tenant ID. To learn more about finding your O365 tenant ID, see https://go.microsoft.com/fwlink/?linkid=2185668

If you disable or don't configure this policy, Microsoft Edge will never send reports about URLs added to a user's local site list to the Site Lists app.

To learn more about Internet Explorer mode, see https://go.microsoft.com/fwlink/?linkid=2165707

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationCloudUserSitesReporting
- GP name: Configure reporting of IE Mode user list entries to the M365 Admin Center Site Lists app
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerIntegrationCloudUserSitesReporting
- Value Type: REG_SZ

Example value:

```
"aba95e58-070f-4784-8dcd-e5fd46c2c6d6"
```

Back to top

InternetExplorerIntegrationComplexNavDataTypes

Configure whether form data and HTTP headers will be sent when entering or exiting Internet Explorer mode

Supported versions:

- On Windows since 96 or later

Description

Starting with Microsoft Edge version 96, navigations that switch between Internet Explorer mode and Microsoft Edge will include form data.

If you enable this policy, you can specify which data types should be included in navigations between Microsoft Edge and Internet Explorer mode.

If you disable or don't configure this policy, Microsoft Edge will use the new behavior of including form data in navigations that change modes.

To learn more, see https://go.microsoft.com/fwlink/?linkid=2174004

Policy options mapping:

- IncludeNone (0) = Do not send form data or headers
- IncludeFormDataOnly (1) = Send form data only
- IncludeHeadersOnly (2) = Send additional headers only
- IncludeFormDataAndHeaders (3) = Send form data and additional headers

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationComplexNavDataTypes
- GP name: Configure whether form data and HTTP headers will be sent when entering or exiting Internet Explorer mode
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerIntegrationComplexNavDataTypes
- Value Type: REG_DWORD

Example value:

```
0x00000003
```

Back to top

InternetExplorerIntegrationEnhancedHangDetection

Configure enhanced hang detection for Internet Explorer mode

Supported versions:

- On Windows since 84 or later

Description

Enhanced hang detection is a more granular approach to detecting hung webpages in Internet Explorer mode than what standalone Internet Explorer uses. When a hung webpage is detected, the browser will apply a mitigation to prevent the rest of the browser from hanging.

This setting allows you to configure the use of enhanced hang detection in case you run into incompatible issues with any of your websites. We recommend disabling this policy only if you see notifications such as "(website) is not responding" in Internet Explorer mode but not in standalone Internet Explorer.

This setting works in conjunction with: InternetExplorerIntegrationLevel is set to 'IEMode' and InternetExplorerIntegrationSiteList policy where the list has at least one entry.

If you set this policy to 'Enabled' or don't configure it, websites running in Internet Explorer mode will use enhanced hang detection.

If you set this policy to 'Disabled', enhanced hang detection is disabled, and users will get the basic Internet Explorer hang detection behavior.

To learn more about Internet Explorer mode, see https://go.microsoft.com/fwlink/?linkid=2094210

Policy options mapping:

- Disabled (0) = Enhanced hang detection disabled
- Enabled (1) = Enhanced hang detection enabled

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationEnhancedHangDetection
- GP name: Configure enhanced hang detection for Internet Explorer mode
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A

- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerIntegrationEnhancedHangDetection
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

InternetExplorerIntegrationLevel

Configure Internet Explorer integration

Supported versions:

- On Windows since 77 or later

Description

For guidance about configuring the optimal experience for Internet Explorer mode see https://go.microsoft.com/fwlink/?linkid=2094210

Policy options mapping:

- None (0) = None
- IEMode (1) = Internet Explorer mode
- NeedIE (2) = Internet Explorer 11

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationLevel
- GP name: Configure Internet Explorer integration
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerIntegrationLevel
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

InternetExplorerIntegrationLocalFileAllowed

Allow launching of local files in Internet Explorer mode

Supported versions:

- On Windows since 88 or later

Description

This policy controls the availability of the --ie-mode-file-url command line argument which is used to launch Microsoft Edge with a local file specified on the command line into Internet Explorer mode.

This setting works in conjunction with: InternetExplorerIntegrationLevel is set to 'IEMode'.

If you set this policy to true, or don't configure it, the user is allowed to use the --ie-mode-file-url command line argument for launching local files in Internet Explorer mode.

If you set this policy to false, the user isn't allowed to use the --ie-mode-file-url command line argument for launching local files in Internet Explorer mode.

To learn more about Internet Explorer mode, see https://go.microsoft.com/fwlink/?linkid=2094210

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationLocalFileAllowed
- GP name: Allow launching of local files in Internet Explorer mode
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerIntegrationLocalFileAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

InternetExplorerIntegrationLocalFileExtensionAllowList

Open local files in Internet Explorer mode file extension allow list

Supported versions:

- On Windows since 88 or later

Description

This policy limits which file:// URLs are allowed to be launched into Internet Explorer mode based on file extension.

This setting works in conjunction with: InternetExplorerIntegrationLevel is set to 'IEMode'.

When a file:// URL is requested to launch in Internet Explorer mode, the file extension of the URL must be present in this list in order for the URL to be allowed to launch in Internet Explorer mode. A URL which is blocked from opening in Internet Explorer mode will instead open in Edge mode.

If you set this policy to the special value "*" or don't configure it, all file extensions are allowed.

To learn more about Internet Explorer mode, see https://go.microsoft.com/fwlink/?linkid=2094210

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationLocalFileExtensionAllowList
- GP name: Open local files in Internet Explorer mode file extension allow list
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\InternetExplorerIntegrationLocalFileExtensionAllowList
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\InternetExplorerIntegrationLocalFileExtensionAllowList\1 = ".mht"
SOFTWARE\Policies\Microsoft\Edge\InternetExplorerIntegrationLocalFileExtensionAllowList\2 = ".pdf"
SOFTWARE\Policies\Microsoft\Edge\InternetExplorerIntegrationLocalFileExtensionAllowList\3 = ".vsdx"
```

Back to top

InternetExplorerIntegrationLocalFileShowContextMenu

Show context menu to open a file:// link in Internet Explorer mode

Supported versions:

- On Windows since 88 or later

Description

This policy controls the visibility of the 'Open link in new Internet Explorer mode tab' option on the context menu for file:// links.

This setting works in conjunction with: InternetExplorerIntegrationLevel is set to 'IEMode'.

If you set this policy to true, the 'Open link in new Internet Explorer mode tab' context menu item will be available for file:// links.

If you set this policy to false or don't configure it, the context menu item will not be added.

If the InternetExplorerIntegrationReloadInIEModeAllowed policy allows users to reload sites in Internet Explorer mode, then the 'Open link in new Internet Explorer mode tab' context menu item will be available for all links, except links to sites explicitly configured by the site list to use Microsoft Edge mode. In this case, if you set this policy to true, the context menu item will be available for file:// links even for sites configured to use Microsoft Edge mode. If you set this policy to false or don't configure it, this policy has no effect.

To learn more about Internet Explorer mode, see https://go.microsoft.com/fwlink/?linkid=2094210

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationLocalFileShowContextMenu
- GP name: Show context menu to open a file:// link in Internet Explorer mode
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerIntegrationLocalFileShowContextMenu
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

InternetExplorerIntegrationLocalMhtFileAllowed

Allow local MHTML files to open automatically in Internet Explorer mode

Supported versions:

- On Windows since 107 or later

Description

This policy controls whether local mht or mhtml files launched from the command line can open automatically in Internet Explorer mode based on the file content without specifying the --ie-mode-file-url command line.

This setting works in conjunction with: InternetExplorerIntegrationLevel is set to 'IEMode' and InternetExplorerIntegrationLocalFileAllowed is enabled or not configured.

If you enable or don't configure this policy, local mht or mhtml files can launch in Microsoft Edge or Internet Explorer mode to best view the file.

If you disable this policy, local mht or mhtml files will launch in Microsoft Edge.

Note that if you use the --ie-mode-file-url command line argument for launching local mht or mhtml files, it takes precedence over how you configured this policy.

To learn more about Internet Explorer mode, see https://go.microsoft.com/fwlink/?linkid=2094210

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationLocalMhtFileAllowed
- GP name: Allow local MHTML files to open automatically in Internet Explorer mode
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerIntegrationLocalMhtFileAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

InternetExplorerIntegrationLocalSiteListExpirationDays

Specify the number of days that a site remains on the local IE mode site list

Supported versions:

- On Windows since 92 or later

Description

If the InternetExplorerIntegrationReloadInIEModeAllowed policy is enabled or not configured, users will be able to tell Microsoft Edge to load specific pages in Internet Explorer mode for a limited number of days.

You can use this setting to determine how many days that configuration is remembered in the browser. After this period has elapsed, the individual page will no longer automatically load in IE mode.

If you disable the InternetExplorerIntegrationReloadInIEModeAllowed policy, this policy has no effect.

If you disable or don't configure this policy, the default value of 30 days is used.

If you enable this policy, you must enter the number of days for which the sites are retained on the user's local site list in Microsoft Edge. The value can be from 0 to 90 days.

To learn more about Internet Explorer mode, see https://go.microsoft.com/fwlink/?linkid=2094210

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationLocalSiteListExpirationDays
- GP name: Specify the number of days that a site remains on the local IE mode site list
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerIntegrationLocalSiteListExpirationDays
- Value Type: REG_DWORD

Example value:

```
0x0000001e
```

Back to top

InternetExplorerIntegrationReloadInIEModeAllowed

Allow unconfigured sites to be reloaded in Internet Explorer mode

Supported versions:

- On Windows since 92 or later

Description

This policy allows users to reload unconfigured sites (that are not configured in the Enterprise Mode Site List) in Internet Explorer mode when browsing in Microsoft Edge and a site requires Internet Explorer for compatibility.

After a site has been reloaded in Internet Explorer mode, "in-page" navigations will stay in Internet Explorer mode (for example, a link, script, or form on the page, or a server-side redirect from another "in-page" navigation). Users can choose to exit from Internet Explorer mode, or Microsoft Edge will automatically exit from Internet Explorer mode when a navigation that isn't "in-page" occurs (for example, using the address bar, the back button, or a favorite link).

Users can also optionally tell Microsoft Edge to use Internet Explorer mode for the site in the future. This choice will be remembered for a length of time managed by the InternetExplorerIntegrationLocalSiteListExpirationDays policy.

If the InternetExplorerIntegrationLevel policy is set to 'IEMode', then sites explicitly configured by the InternetExplorerIntegrationSiteList policy's site list to use Microsoft Edge can't be reloaded in Internet Explorer mode, and sites configured by the site list or by the SendIntranetToInternetExplorer policy to use Internet Explorer mode can't exit from Internet Explorer mode.

If you enable this policy, users are allowed to reload unconfigured sites in Internet Explorer mode.

If you disable this policy, users aren't allowed to reload unconfigured sites in Internet Explorer mode.

Note that if you enable this policy, it takes precedence over how you configured the InternetExplorerIntegrationTestingAllowed policy, and that policy will be disabled.

To learn more about Internet Explorer mode, see https://go.microsoft.com/fwlink/?linkid=2094210

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationReloadInIEModeAllowed
- GP name: Allow unconfigured sites to be reloaded in Internet Explorer mode
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: InternetExplorerIntegrationReloadInIEModeAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

InternetExplorerIntegrationSiteList

Configure the Enterprise Mode Site List

Supported versions:

- On Windows since 78 or later

Description

For guidance about configuring the optimal experience for Internet Explorer mode see https://go.microsoft.com/fwlink/?linkid=2094210

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationSiteList
- GP name: Configure the Enterprise Mode Site List
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerIntegrationSiteList
- Value Type: REG_SZ

Example value:

```
"https://internal.contoso.com/sitelist.xml"
```

Back to top

InternetExplorerIntegrationSiteListRefreshInterval

Configure how frequently the Enterprise Mode Site List is refreshed

Supported versions:

- On Windows since 93 or later

Description

This setting lets you specify a custom refresh interval for the Enterprise Mode Site List. The refresh interval is specified in minutes. The minimum refresh interval is 30 minutes.

This setting is applicable only when the InternetExplorerIntegrationSiteList or InternetExplorerIntegrationCloudSiteList setting is configured.

If you configure this policy, Microsoft Edge will attempt to retrieve an updated version of the configured Enterprise Mode Site List using the specified refresh interval.

If you disable or don't configure this policy, Microsoft Edge will use a default refresh interval, currently 120 minutes.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationSiteListRefreshInterval
- GP name: Configure how frequently the Enterprise Mode Site List is refreshed
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerIntegrationSiteListRefreshInterval
- Value Type: REG_DWORD

Example value:

```
0x000000f0
```

Back to top

InternetExplorerIntegrationSiteRedirect

Specify how "in-page" navigations to unconfigured sites behave when started from Internet Explorer mode pages

Supported versions:

- On Windows since 81 or later

Description

An "in-page" navigation is started from a link, a script, or a form on the current page. It can also be a server-side redirect of a previous "in-page" navigation attempt. Conversely, a user can start a navigation that isn't "in-page" that's independent of the current page in several ways by using the browser controls. For example, using the address bar, the back button, or a favorite link.

This setting lets you specify whether navigations from pages loaded in Internet Explorer mode to unconfigured sites (that are not configured in the Enterprise Mode Site List) switch back to Microsoft Edge or remain in Internet Explorer mode.

This setting works in conjunction with: InternetExplorerIntegrationLevel is set to 'IEMode' and InternetExplorerIntegrationSiteList policy where the list has at least one entry.

If you disable or don't configure this policy, only sites configured to open in Internet Explorer mode will open in that mode. Any site not configured to open in Internet Explorer mode will be redirected back to Microsoft Edge.

If you set this policy to 'Default', only sites configured to open in Internet Explorer mode will open in that mode. Any site not configured to open in Internet Explorer mode will be redirected back to Microsoft Edge.

If you set this policy to 'AutomaticNavigationsOnly', you get the default experience except that all automatic navigations (such as 302 redirects) to unconfigured sites will be kept in Internet Explorer mode.

If you set this policy to 'AllInPageNavigations', all navigations from pages loaded in IE mode to unconfigured sites are kept in Internet Explorer mode (Least Recommended).

If the InternetExplorerIntegrationReloadInIEModeAllowed policy allows users to reload sites in Internet Explorer mode, then all in-page navigations from unconfigured sites that users have chosen to reload in Internet Explorer mode will be kept in Internet Explorer mode, regardless of how this policy is configured.

To learn more about Internet Explorer mode, see https://go.microsoft.com/fwlink/?linkid=2105106

Policy options mapping:

- Default (0) = Default
- AutomaticNavigationsOnly (1) = Keep only automatic navigations in Internet Explorer mode
- AllInPageNavigations (2) = Keep all in-page navigations in Internet Explorer mode

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationSiteRedirect
- GP name: Specify how "in-page" navigations to unconfigured sites behave when started from Internet Explorer mode pages
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge

- Path (Recommended): N/A
- Value Name: InternetExplorerIntegrationSiteRedirect
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

InternetExplorerIntegrationTestingAllowed

Allow Internet Explorer mode testing (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 94.

Supported versions:

- On Windows since 86, until 94

Description

This policy is obsolete because it has been superseded by an improved feature. It doesn't work in Microsoft Edge after version 94. To allow users to open applications in Internet Explorer mode, use the InternetExplorerIntegrationReloadInIEModeAllowed policy instead. Alternatively, users can still use the --ie-mode-test flag.

This policy allows users to test applications in Internet Explorer mode by opening an Internet Explorer mode tab in Microsoft Edge.

Users can do so from within the "More tools" menu by selecting 'Open sites in Internet Explorer mode'.

Additionally, users can test their applications in a modern browser without removing applications from the site list using the option 'Open sites in Edge mode'.

This setting works in conjunction with: InternetExplorerIntegrationLevel is set to 'IEMode'.

If you enable this policy, the option to 'Open sites in Internet Explorer mode' will be visible under "More tools". Users can view their sites in Internet Explorer mode on this tab. Another option to 'Open sites in Edge mode' will also be visible under "More tools" to help testing sites in a modern browser without removing them from the site list. Note that if the InternetExplorerIntegrationReloadInIEModeAllowed policy is enabled, it takes precedence and these options will not be visible under "More tools".

If you disable or don't configure this policy, users can't see the options 'Open in Internet Explorer mode' and 'Open in Edge mode' under "More tools" menu. However, users can configure these options with the --ie-mode-test flag.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationTestingAllowed
- GP name: Allow Internet Explorer mode testing (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/

- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerIntegrationTestingAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

InternetExplorerIntegrationWindowOpenHeightAdjustment

Configure the pixel adjustment between window.open heights sourced from IE mode pages vs. Edge mode pages

Supported versions:

- On Windows since 95 or later

Description

This setting lets you specify a custom adjustment to the height of popup windows generated via window.open from the Internet Explorer mode site.

If you configure this policy, Microsoft Edge will add the adjustment value to the height, in pixels. The exact difference depends on the UI configuration of both IE and Edge, but a typical difference is 5.

If you disable or don't configure this policy, Microsoft Edge will treat IE mode window.open the same as Edge mode window.open in window height calculations.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationWindowOpenHeightAdjustment
- GP name: Configure the pixel adjustment between window.open heights sourced from IE mode pages vs. Edge mode pages
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerIntegrationWindowOpenHeightAdjustment
- Value Type: REG_DWORD

Example value:

```
0x00000005
```

Back to top

InternetExplorerIntegrationWindowOpenWidthAdjustment

Configure the pixel adjustment between window.open widths sourced from IE mode pages vs. Edge mode pages

Supported versions:

- On Windows since 95 or later

Description

This setting lets you specify a custom adjustment to the width of popup windows generated via window.open from the Internet Explorer mode site.

If you configure this policy, Microsoft Edge will add the adjustment value to the width, in pixels. The exact difference depends on the UI configuration of both IE and Edge, but a typical difference is 4.

If you disable or don't configure this policy, Microsoft Edge will treat IE mode window.open the same as Edge mode window.open in window width calculations.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerIntegrationWindowOpenWidthAdjustment
- GP name: Configure the pixel adjustment between window.open widths sourced from IE mode pages vs. Edge mode pages
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerIntegrationWindowOpenWidthAdjustment
- Value Type: REG_DWORD

Example value:

```
0x00000004
```

Back to top

InternetExplorerModeEnableSavePageAs

Allow Save page as in Internet Explorer mode

Supported versions:

- On Windows since 101 or later

Description

This policy enables 'Save page as' functionality in Internet Explorer mode. Users can use this option to save the current page in the browser. When a user re-opens a saved page, it will be loaded in the default browser.

If you enable this policy, the "Save page as" option will be clickable in "More tools".

If you disable or don't configure this policy, users can't select the "Save page as" option in "More tools".

Note: To make the "Ctrl+S" shortcut work, users must enable the Internet Explorer policy, 'Enable extended hot key in Internet Explorer mode'.

To learn more about Internet Explorer mode, see https://go.microsoft.com/fwlink/?linkid=2094210

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerModeEnableSavePageAs
- GP name: Allow Save page as in Internet Explorer mode
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerModeEnableSavePageAs
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

InternetExplorerModeTabInEdgeModeAllowed

Allow sites configured for Internet Explorer mode to open in Microsoft Edge

Supported versions:

- On Windows since 97 or later

Description

This policy lets sites configured to open in Internet Explorer mode to be opened by Microsoft Edge for testing on a modern browser without removing them from the site list.

Users can configure this setting in the "More tools" menu by selecting 'Open sites in Microsoft Edge'.

If you enable this policy, the option to 'Open sites in Microsoft Edge' will be visible under "More tools". Users use this option to test IE mode sites on a modern browser.

If you disable or don't configure this policy, users can't see the option 'Open in Microsoft Edge' under the "More tools" menu. However, users can access this menu option with the --ie-mode-test flag.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerModeTabInEdgeModeAllowed
- GP name: Allow sites configured for Internet Explorer mode to open in Microsoft Edge
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerModeTabInEdgeModeAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

InternetExplorerModeToolbarButtonEnabled

Show the Reload in Internet Explorer mode button in the toolbar

Supported versions:

- On Windows since 96 or later

Description

Set this policy to show the Reload in Internet Explorer mode button in the toolbar. Users can hide the button in the toolbar through edge://settings/appearance. The button will only be shown on the toolbar when the InternetExplorerIntegrationReloadInIEModeAllowed policy is enabled or if the user has chosen to enable "Allow sites to be reloaded in Internet Explorer mode".

If you enable this policy, the Reload in Internet mode button is pinned to the toolbar.

If you disable or don't configure this policy, the Reload in Internet Explorer mode button isn't shown in the toolbar by default. Users can toggle the Show Internet Explorer mode button in edge://settings/appearance.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerModeToolbarButtonEnabled
- GP name: Show the Reload in Internet Explorer mode button in the toolbar
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: InternetExplorerModeToolbarButtonEnabled

- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

InternetExplorerZoomDisplay

Display zoom in IE Mode tabs with DPI Scale included like it is in Internet Explorer

Supported versions:

- On Windows since 103 or later

Description

Lets you display zoom in IE Mode tabs similar to how it was displayed in Internet Explorer, where the DPI scale of the display is factored in.

For example, if you have a page zoomed to 200% on a 100 DPI scale display and you change the display to 150 DPI, Microsoft Edge would still display the zoom as 200%. However, Internet Explorer factors in the DPI scale and displays 300%.

If you enable this policy, zoom values will be displayed with the DPI scale included for IE Mode tabs.

If you disable or don't configure this policy, zoom values will be displayed without DPI scale included for IE Mode tabs

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InternetExplorerZoomDisplay
- GP name: Display zoom in IE Mode tabs with DPI Scale included like it is in Internet Explorer
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: InternetExplorerZoomDisplay
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

IntranetRedirectBehavior

Intranet Redirection Behavior

Supported versions:

- On Windows and macOS since 88 or later

Description

This policy configures behavior for intranet redirection via DNS interception checks. The checks attempt to discover whether the browser is behind a proxy that redirects unknown host names.

If this policy isn't configured, the browser will use the default behavior of DNS interception checks and intranet redirect suggestions. In M88, they are enabled by default but will be disabled by default in the future release.

DNSInterceptionChecksEnabled is a related policy that might also disable DNS interception checks. However, this policy is a more flexible version which might separately control intranet redirection infobars and might be expanded in the future. If either DNSInterceptionChecksEnabled or this policy make a request to disable interception checks, the checks will be disabled. If DNS interception checks are disabled by this policy but GoToIntranetSiteForSingleWordEntryInAddressBar is enabled, single word queries will still result in intranet navigations.

Policy options mapping:

- Default (0) = Use default browser behavior.
- DisableInterceptionChecksDisableInfobar (1) = Disable DNS interception checks and did-you-mean "http://intranetsite/" infobars.
- DisableInterceptionChecksEnableInfobar (2) = Disable DNS interception checks; allow did-you-mean "http://intranetsite/" infobars.
- EnableInterceptionChecksEnableInfobar (3) = Allow DNS interception checks and did-you-mean "http://intranetsite/" infobars.

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: IntranetRedirectBehavior
- GP name: Intranet Redirection Behavior
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: IntranetRedirectBehavior
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: IntranetRedirectBehavior
- Example value:

```
<integer>1</integer>
```

Back to top

IsolateOrigins

Enable site isolation for specific origins

Supported versions:

- On Windows and macOS since 77 or later

Description

Specify origins to run in an isolated process.

By default, Microsoft Edge isolates pages from each Site into its own process. This policy enables more granular isolation based on Origin rather than Site. For example, specifying https://subdomain.contoso.com/ will cause pages from https://subdomain.contoso.com/ to be isolated in a different process than pages from other Origins within the https://contoso.com/ Site.

If you enable this policy, each of the named origins in a comma-separated list will run in its own process.

If you disable or don't configure this policy, pages will be isolated on a per-Site basis.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: IsolateOrigins
- GP name: Enable site isolation for specific origins
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: IsolateOrigins
- Value Type: REG_SZ

Example value:

```
"https://contoso.com/,https://fabrikam.com/"
```

Mac information and settings

- Preference Key Name: IsolateOrigins
- Example value:

```
<string>https://contoso.com/,https://fabrikam.com/</string>
```

Back to top

LiveCaptionsAllowed

Live captions allowed

Supported versions:

- On Windows since 103 or later

Description

Allow users to turn the Live captions feature on or off.

Live captions is an accessibility feature that converts speech from the audio that plays in Microsoft Edge in to text and shows this text in a separate window. The entire process happens on the device and no audio or caption text ever leaves the device.

If you enable or don't configure this policy, users can turn this feature on or off at edge://settings/accessibility.

If you disable this policy, users will not be able to turn this accessibility feature on. If speech recognition files have been downloaded previously, they will be deleted from the device in 30 days. We recommend avoiding this option unless it's needed in your environment.

If users choose to turn on Live captions, speech recognition files (approximately 100 megabytes) will be downloaded to the device on first run and then periodically to improve performance and accuracy. These files will be deleted after 30 days.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: LiveCaptionsAllowed
- GP name: Live captions allowed
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: LiveCaptionsAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

LocalBrowserDataShareEnabled

Enable Windows to search local Microsoft Edge browsing data

Supported versions:

- On Windows since 93 or later

Description

Enables Windows to index Microsoft Edge browsing data stored locally on the user's device and allows users to find and launch previously stored browsing data directly from Windows features such as the search box on the taskbar in Windows.

If you enable this policy or don't configure it, Microsoft Edge will publish local browsing data to the Windows Indexer.

If you disable this policy, Microsoft Edge will not share data to the Windows Indexer.

Note that if you disable this policy, Microsoft Edge will remove the data shared with Windows on the device and stop sharing any new browsing data.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: LocalBrowserDataShareEnabled
- GP name: Enable Windows to search local Microsoft Edge browsing data
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: LocalBrowserDataShareEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

LocalProvidersEnabled

Allow suggestions from local providers

Supported versions:

- On Windows and macOS since 83 or later

Description

Allow suggestions from suggestion providers on the device (local providers), for example, Favorites and Browsing History, in Microsoft Edge's Address Bar and Auto-Suggest List.

If you enable this policy, suggestions from local providers are used.

If you disable this policy, suggestions from local providers are never used. Local history and local favorites suggestions will not appear.

If you do not configure this policy, suggestions from local providers are allowed but the user can change that using the settings toggle.

Note that some features may not be available if a policy to disable this feature has been applied. For example,

Browsing History suggestions will not be available if you enable the SavingBrowserHistoryDisabled policy.

This policy requires a browser restart to finish applying.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: LocalProvidersEnabled
- GP name: Allow suggestions from local providers
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: LocalProvidersEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: LocalProvidersEnabled
- Example value:

```
<false/>
```

Back to top

MAUEnabled

Always use Microsoft AutoUpdate as the updater for Microsoft Edge

Supported versions:

- On macOS since 93 or later

Description

This policy lets you configure the updater that Microsoft Edge uses.

If you enable this policy, Microsoft Edge will only be updated by Microsoft AutoUpdate.

If you disable or don't configure this policy, Microsoft Edge will be updated by Microsoft Edge Update.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Mac information and settings

- Preference Key Name: MAUEnabled
- Example value:

```
<true/>
```

Back to top

MSAWebSiteSSOUsingThisProfileAllowed

Allow single sign-on for Microsoft personal sites using this profile

Supported versions:

- On Windows and macOS since 93 or later

Description

'Allow single sign-on for Microsoft personal sites using this profile' option allows non-MSA profiles to be able to use single sign-on for Microsoft sites using MSA credentials present on the machine. This option shows up for end-users as a toggle in Settings -> Profiles -> Profile Preferences for non-MSA profiles only.

If you disable this policy, non-MSA profiles will not be able to use single sign-on for Microsoft sites using MSA credentials present on the machine.

If you enable this policy or don't configure it, users will be able to use the Settings option to ensure non-MSA profiles are able to use single sign-on for Microsoft sites using MSA credentials present on the machine provided only a single MSA account exists on the machine.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: MSAWebSiteSSOUsingThisProfileAllowed
- GP name: Allow single sign-on for Microsoft personal sites using this profile
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: MSAWebSiteSSOUsingThisProfileAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: MSAWebSiteSSOUsingThisProfileAllowed
- Example value:

```
<false/>
```

Back to top

ManagedConfigurationPerOrigin

Sets managed configuration values for websites to specific origins

Supported versions:

- On Windows and macOS since 90 or later

Description

Setting this policy defines the return value of Managed Configuration API for given origin.

Managed Configuration API is a key-value configuration that can be accessed via navigator.device.getManagedConfiguration() javascript call. This API is only available to origins which correspond to force-installed web applications via WebAppInstallForceList.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Dictionary

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ManagedConfigurationPerOrigin
- GP name: Sets managed configuration values for websites to specific origins
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ManagedConfigurationPerOrigin
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ManagedConfigurationPerOrigin = [
  {
    "managed_configuration_hash": "asd891jedasd12ue9h",
    "managed_configuration_url": "https://static.contoso.com/configuration.json",
    "origin": "https://www.contoso.com"
  },
  {
    "managed_configuration_hash": "djio12easd89u12aws",
    "managed_configuration_url": "https://static.contoso.com/configuration2.json",
    "origin": "https://www.example.com"
  }
]
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\ManagedConfigurationPerOrigin = [{"managed_configuration_hash":
"asd891jedasd12ue9h", "managed_configuration_url": "https://static.contoso.com/configuration.json",
"origin": "https://www.contoso.com"}, {"managed_configuration_hash": "djio12easd89u12aws",
"managed_configuration_url": "https://static.contoso.com/configuration2.json", "origin":
"https://www.example.com"}]
```

Mac information and settings

- Preference Key Name: ManagedConfigurationPerOrigin
- Example value:

```
<key>ManagedConfigurationPerOrigin</key>
<array>
  <dict>
    <key>managed_configuration_hash</key>
    <string>asd891jedasd12ue9h</string>
    <key>managed_configuration_url</key>
    <string>https://static.contoso.com/configuration.json</string>
    <key>origin</key>
    <string>https://www.contoso.com</string>
  </dict>
  <dict>
    <key>managed_configuration_hash</key>
    <string>djio12easd89u12aws</string>
    <key>managed_configuration_url</key>
    <string>https://static.contoso.com/configuration2.json</string>
    <key>origin</key>
    <string>https://www.example.com</string>
  </dict>
</array>
```

Back to top

ManagedFavorites

Configure favorites

Supported versions:

- On Windows and macOS since 77 or later

Description

Configures a list of managed favorites.

The policy creates a list of favorites. Each favorite contains the keys "name" and "url," which hold the favorite's name and its target. You can configure a subfolder by defining a favorites without an "url" key but with an additional "children" key that contains a list of favorites as defined above (some of which may be folders again). Microsoft Edge amends incomplete URLs as if they were submitted via the Address Bar, for example "microsoft.com" becomes "https://microsoft.com/".

These favorites are placed in a folder that can't be modified by the user (but the user can choose to hide it from the favorites bar). By default the folder name is "Managed favorites" but you can change it by adding to the list of favorites a dictionary containing the key "toplevel_name" with the desired folder name as the value.

Managed favorites are not synced to the user account and can't be modified by extensions.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Dictionary

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ManagedFavorites
- GP name: Configure favorites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ManagedFavorites
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ManagedFavorites = [
  {
    "toplevel_name": "My managed favorites folder"
  },
  {
    "name": "Microsoft",
    "url": "microsoft.com"
  },
  {
    "name": "Bing",
    "url": "bing.com"
  },
  {
    "children": [
      {
        "name": "Microsoft Edge Insiders",
        "url": "www.microsoftedgeinsider.com"
      },
      {
        "name": "Microsoft Edge",
        "url": "www.microsoft.com/windows/microsoft-edge"
      }
    ],
    "name": "Microsoft Edge links"
  }
]
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\ManagedFavorites = [{"toplevel_name": "My managed favorites folder"},
{"name": "Microsoft", "url": "microsoft.com"}, {"name": "Bing", "url": "bing.com"}, {"children": [{"name":
"Microsoft Edge Insiders", "url": "www.microsoftedgeinsider.com"}, {"name": "Microsoft Edge", "url":
"www.microsoft.com/windows/microsoft-edge"}], "name": "Microsoft Edge links"}]
```

Mac information and settings

- Preference Key Name: ManagedFavorites
- Example value:

```
<key>ManagedFavorites</key>
<array>
  <dict>
    <key>toplevel_name</key>
    <string>My managed favorites folder</string>
  </dict>
  <dict>
    <key>name</key>
    <string>Microsoft</string>
    <key>url</key>
    <string>microsoft.com</string>
  </dict>
  <dict>
    <key>name</key>
    <string>Bing</string>
    <key>url</key>
    <string>bing.com</string>
  </dict>
  <dict>
    <key>children</key>
    <array>
      <dict>
        <key>name</key>
        <string>Microsoft Edge Insiders</string>
        <key>url</key>
        <string>www.microsoftedgeinsider.com</string>
      </dict>
      <dict>
        <key>name</key>
        <string>Microsoft Edge</string>
        <key>url</key>
        <string>www.microsoft.com/windows/microsoft-edge</string>
      </dict>
    </array>
    <key>name</key>
    <string>Microsoft Edge links</string>
  </dict>
</array>
```

Back to top

ManagedSearchEngines

Manage Search Engines

Supported versions:

- On Windows and macOS since 77 or later

Description

Lets you configure a list of up to 10 search engines, one of which must be marked as the default search engine. Starting in Microsoft Edge version 100, you can configure up to 100 engines.

You do not need to specify the encoding. Starting in Microsoft Edge 80, the suggest_url and image_search_url parameters are optional. The optional parameter, image_search_post_params (consists of comma-separated name/value pairs), is available starting in Microsoft Edge 80.

Starting in Microsoft Edge 83, you can enable search engine discovery with the optional allow_search_engine_discovery parameter. This parameter must be the first item in the list. If allow_search_engine_discovery isn't specified, search engine discovery will be disabled by default. Starting in Microsoft Edge 84, you can set this policy as a recommended policy to allow search provider discovery. You don't need to add the optional allow_search_engine_discovery parameter. Starting in Microsoft Edge 100, setting this policy as a recommended policy will also allow users to manually add new search engines from their Microsoft Edge settings.

If you enable this policy, users can't add, remove, or change any search engine in the list. Users can set their default search engine to any search engine in the list.

If you disable or don't configure this policy, users can modify the search engines list as desired.

If the DefaultSearchProviderSearchURL policy is set, this policy (ManagedSearchEngines) is ignored. The user must restart their browser to finish applying this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Dictionary

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ManagedSearchEngines
- GP name: Manage Search Engines
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ManagedSearchEngines
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\ManagedSearchEngines = [
  {
    "allow_search_engine_discovery": true
  },
  {
    "is_default": true,
    "keyword": "example1.com",
    "name": "Example1",
    "search_url": "https://www.example1.com/search?q={searchTerms}",
    "suggest_url": "https://www.example1.com/qbox?query={searchTerms}"
  },
  {
    "image_search_post_params": "content={imageThumbnail},url={imageURL},sbisrc={SearchSource}",
    "image_search_url": "https://www.example2.com/images/detail/search?iss=sbiupload",
    "keyword": "example2.com",
    "name": "Example2",
    "search_url": "https://www.example2.com/search?q={searchTerms}",
    "suggest_url": "https://www.example2.com/qbox?query={searchTerms}"
  },
  {
    "encoding": "UTF-8",
    "image_search_url": "https://www.example3.com/images/detail/search?iss=sbiupload",
    "keyword": "example3.com",
    "name": "Example3",
    "search_url": "https://www.example3.com/search?q={searchTerms}",
    "suggest_url": "https://www.example3.com/qbox?query={searchTerms}"
  },
  {
    "keyword": "example4.com",
    "name": "Example4",
    "search_url": "https://www.example4.com/search?q={searchTerms}"
  }
]
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\ManagedSearchEngines = [{"allow_search_engine_discovery": true},
{"is_default": true, "keyword": "example1.com", "name": "Example1", "search_url":
"https://www.example1.com/search?q={searchTerms}", "suggest_url": "https://www.example1.com/qbox?query=
{searchTerms}"}, {"image_search_post_params": "content={imageThumbnail},url={imageURL},sbisrc=
{SearchSource}", "image_search_url": "https://www.example2.com/images/detail/search?iss=sbiupload",
"keyword": "example2.com", "name": "Example2", "search_url": "https://www.example2.com/search?q=
{searchTerms}", "suggest_url": "https://www.example2.com/qbox?query={searchTerms}"}, {"encoding": "UTF-8",
"image_search_url": "https://www.example3.com/images/detail/search?iss=sbiupload", "keyword":
"example3.com", "name": "Example3", "search_url": "https://www.example3.com/search?q={searchTerms}",
"suggest_url": "https://www.example3.com/qbox?query={searchTerms}"}, {"keyword": "example4.com", "name":
"Example4", "search_url": "https://www.example4.com/search?q={searchTerms}"}]
```

Mac information and settings

- Preference Key Name: ManagedSearchEngines
- Example value:

```
<key>ManagedSearchEngines</key>
<array>
  <dict>
    <key>allow_search_engine_discovery</key>
    <true/>
  </dict>
  <dict>
    <key>is_default</key>
    <true/>
    <key>keyword</key>
    <string>example1.com</string>
    <key>name</key>
    <string>Example1</string>
    <key>search_url</key>
    <string>https://www.example1.com/search?q={searchTerms}</string>
    <key>suggest_url</key>
    <string>https://www.example1.com/qbox?query={searchTerms}</string>
  </dict>
  <dict>
    <key>image_search_post_params</key>
    <string>content={imageThumbnail},url={imageURL},sbisrc={SearchSource}</string>
    <key>image_search_url</key>
    <string>https://www.example2.com/images/detail/search?iss=sbiupload</string>
    <key>keyword</key>
    <string>example2.com</string>
    <key>name</key>
    <string>Example2</string>
    <key>search_url</key>
    <string>https://www.example2.com/search?q={searchTerms}</string>
    <key>suggest_url</key>
    <string>https://www.example2.com/qbox?query={searchTerms}</string>
  </dict>
  <dict>
    <key>encoding</key>
    <string>UTF-8</string>
    <key>image_search_url</key>
    <string>https://www.example3.com/images/detail/search?iss=sbiupload</string>
    <key>keyword</key>
    <string>example3.com</string>
    <key>name</key>
    <string>Example3</string>
    <key>search_url</key>
    <string>https://www.example3.com/search?q={searchTerms}</string>
    <key>suggest_url</key>
    <string>https://www.example3.com/qbox?query={searchTerms}</string>
  </dict>
  <dict>
    <key>keyword</key>
    <string>example4.com</string>
    <key>name</key>
    <string>Example4</string>
    <key>search_url</key>
    <string>https://www.example4.com/search?q={searchTerms}</string>
  </dict>
</array>
```

Back to top

MathSolverEnabled

Let users snip a Math problem and get the solution with a step-by-step explanation in Microsoft Edge

Supported versions:

- On Windows and macOS since 91 or later

Description

This policy lets you manage whether users can use the Math Solver tool in Microsoft Edge or not.

If you enable or don't configure the policy, then a user can take a snip of the Math problem and get the solution including a step-by-step explanation of the solution in a Microsoft Edge side pane.

If you disable the policy, then the Math Solver tool will be disabled and users will not be able to use it.

Note: Setting the ComponentUpdatesEnabled policy to disabled will also disable the Math Solver component.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: MathSolverEnabled
- GP name: Let users snip a Math problem and get the solution with a step-by-step explanation in Microsoft Edge
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: MathSolverEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: MathSolverEnabled
- Example value:

```
<true/>
```

Back to top

MaxConnectionsPerProxy

Maximum number of concurrent connections to the proxy server

Supported versions:

- On Windows and macOS since 77 or later

Description

Specifies the maximum number of simultaneous connections to the proxy server.

Some proxy servers can't handle a high number of concurrent connections per client - you can solve this by setting this policy to a lower value.

The value of this policy should be lower than 100 and higher than 6. The default value is 32.

Some web apps are known to consume many connections with hanging GETs - lowering the maximum connections below 32 may lead to browser networking hangs if too many of these kind of web apps are open.

If you don't configure this policy, the default value (32) is used.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: MaxConnectionsPerProxy
- GP name: Maximum number of concurrent connections to the proxy server
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: MaxConnectionsPerProxy
- Value Type: REG_DWORD

Example value:

```
0x00000020
```

Mac information and settings

- Preference Key Name: MaxConnectionsPerProxy
- Example value:

```
<integer>32</integer>
```

Back to top

MediaRouterCastAllowAllIPs

Allow Google Cast to connect to Cast devices on all IP addresses

Supported versions:

- On Windows and macOS since 77 or later

Description

Enable this policy to let Google Cast connect to Cast devices on all IP addresses, not just RFC1918/RFC4193 private addresses.

Disable this policy to restrict Google Cast to Cast devices on RFC1918/RFC4193 private addresses.

If you don't configure this policy, Google Cast connects to Cast devices on RFC1918/RFC4193 private addresses only, unless you enable the CastAllowAllIPs feature.

If the EnableMediaRouter policy is disabled, then this policy has no effect.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: MediaRouterCastAllowAllIPs
- GP name: Allow Google Cast to connect to Cast devices on all IP addresses
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: MediaRouterCastAllowAllIPs
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: MediaRouterCastAllowAllIPs
- Example value:

```
<false/>
```

Back to top

MetricsReportingEnabled

Enable usage and crash-related data reporting (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 88.

Supported versions:

- On Windows and macOS since 77, until 88

Description

This policy is no longer supported. It is replaced by DiagnosticData (for Windows 7, Windows 8, and macOS) and Allow Telemetry on Win 10 (https://go.microsoft.com/fwlink/?linkid=2099569).

This policy enables reporting of usage and crash-related data about Microsoft Edge to Microsoft.

Enable this policy to send reporting of usage and crash-related data to Microsoft. Disable this policy to not send the data to Microsoft. In both cases, users can't change or override the setting.

On Windows 10, if you don't configure this policy, Microsoft Edge will default to the Windows diagnostic data setting. If you enable this policy, Microsoft Edge will only send usage data if the Windows Diagnostic data setting is set to Enhanced or Full. If you disable this policy, Microsoft Edge will not send usage data. Crash-related data is sent based on the Windows Diagnostic data setting. Learn more about Windows Diagnostic data settings at https://go.microsoft.com/fwlink/?linkid=2099569

On Windows 7, Windows 8, and macOS, this policy controls sending usage and crash-related data. If you don't configure this policy, Microsoft Edge will default to the user's preference.

To enable this policy,SendSiteInfoToImproveServices must be set to Enabled. If MetricsReportingEnabled or

SendSiteInfoToImproveServices is Not Configured or Disabled, this data will not be sent to Microsoft.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management, or macOS instances that are that are managed via MDM or joined to a domain via MCX.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: MetricsReportingEnabled
- GP name: Enable usage and crash-related data reporting (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: MetricsReportingEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: MetricsReportingEnabled
- Example value:

```
<true/>
```

Back to top

MicrosoftEdgeInsiderPromotionEnabled

Microsoft Edge Insider Promotion Enabled

Supported versions:

- On Windows and macOS since 98 or later

Description

Shows content promoting the Microsoft Edge Insider channels on the About Microsoft Edge settings page.

If you enable or don't configure this policy, the Microsoft Edge Insider promotion content will be shown on the About Microsoft Edge page.

If you disable this policy, the Microsoft Edge Insider promotion content will not be shown on the About Microsoft Edge page.

Supported features:

- Can be mandatory: Yes

- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: MicrosoftEdgeInsiderPromotionEnabled
- GP name: Microsoft Edge Insider Promotion Enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: MicrosoftEdgeInsiderPromotionEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: MicrosoftEdgeInsiderPromotionEnabled
- Example value:

```
<true/>
```

Back to top

MicrosoftEditorProofingEnabled

Spell checking provided by Microsoft Editor

Supported versions:

- On Windows and macOS since 105 or later

Description

The Microsoft Editor service provides enhanced spell and grammar checking for editable text fields on web pages.

If you enable or don't configure this policy, Microsoft Editor spell check can be used for eligible text fields.

If you disable this policy, spell check can only be provided by local engines that use platform or Hunspell services. The results from these engines might be less informative than the results Microsoft Editor can provide.

If the SpellcheckEnabled policy is set to disabled, or the user disables spell checking in the settings page, this policy will have no effect.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: MicrosoftEditorProofingEnabled
- GP name: Spell checking provided by Microsoft Editor
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: MicrosoftEditorProofingEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: MicrosoftEditorProofingEnabled
- Example value:

```
<false/>
```

Back to top

MicrosoftEditorSynonymsEnabled

Synonyms are provided when using Microsoft Editor spell checker

Supported versions:

- On Windows and macOS since 105 or later

Description

The Microsoft Editor service provides enhanced spell and grammar checking for editable text fields on web pages, and synonyms can be suggested as an integrated feature.

If you enable this policy, Microsoft Editor spell checker will provide synonyms for suggestions for misspelled words.

If you disable or don't configure this policy, Microsoft Editor spell checker will not provide synonyms for suggestions for misspelled words.

If the SpellcheckEnabled policy or the MicrosoftEditorProofingEnabled policy are set to disabled, or the user disables spell checking or chooses not to use Microsoft Editor spell checker in the settings page, this policy will have no effect.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: MicrosoftEditorSynonymsEnabled

- GP name: Synonyms are provided when using Microsoft Editor spell checker
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: MicrosoftEditorSynonymsEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: MicrosoftEditorSynonymsEnabled
- Example value:

```
<false/>
```

Back to top

MicrosoftOfficeMenuEnabled

Allow users to access the Microsoft Office menu (deprecated)

> DEPRECATED: This policy is deprecated. It is currently supported but will become obsolete in a future release.

Supported versions:

- On Windows and macOS since 100 or later

Description

This policy is deprecated because it's been replaced by the Microsoft Edge sidebar. Microsoft Office applications are now available in the sidebar, which can be managed by HubsSidebarEnabled policy.

When users can access the Microsoft Office menu, they can get access to Office applications such as Microsoft Word and Microsoft Excel.

If you enable or don't configure this policy, users can open the Microsoft Office menu.

If you disable this policy, users won't be able to access the Microsoft Office menu.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: MicrosoftOfficeMenuEnabled
- GP name: Allow users to access the Microsoft Office menu (deprecated)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/

- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: MicrosoftOfficeMenuEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: MicrosoftOfficeMenuEnabled
- Example value:

```
<false/>
```

Back to top

NativeWindowOcclusionEnabled

Enable Native Window Occlusion (deprecated)

> DEPRECATED: This policy is deprecated. It is currently supported but will become obsolete in a future release.

Supported versions:

- On Windows since 84 or later

Description

This policy is deprecated, use the 'WindowOcclusionEnabled' policy instead. It won't work in Microsoft Edge version 92.

Enables native window occlusion in Microsoft Edge.

If you enable this setting, to reduce CPU and power consumption Microsoft Edge will detect when a window is covered by other windows, and will suspend work painting pixels.

If you disable this setting Microsoft Edge will not detect when a window is covered by other windows.

If this policy is left not set, occlusion detection will be enabled.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NativeWindowOcclusionEnabled
- GP name: Enable Native Window Occlusion (deprecated)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/

- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: NativeWindowOcclusionEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

NavigationDelayForInitialSiteListDownloadTimeout

Set a timeout for delay of tab navigation for the Enterprise Mode Site List

Supported versions:

- On Windows since 84 or later

Description

Allows you to set a timeout, in seconds, for Microsoft Edge tabs waiting to navigate until the browser has downloaded the initial Enterprise Mode Site List.

This setting works in conjunction with: InternetExplorerIntegrationLevel is set to 'IEMode' and InternetExplorerIntegrationSiteList policy where the list has at least one entry and DelayNavigationsForInitialSiteListDownload is set to "All eligible navigations" (1).

Tabs will not wait longer than this timeout for the Enterprise Mode Site List to download. If the browser has not finished downloading the Enterprise Mode Site List when the timeout expires, Microsoft Edge tabs will continue navigating anyway. The value of the timeout should be no greater than 20 seconds and no fewer than 1 second.

If you set the timeout in this policy to a value greater than the default of 2 seconds, an information bar is shown to the user after 2 seconds. The information bar contains a button that allows the user to quit waiting for the Enterprise Mode Site List download to complete.

If you don't configure this policy, the default timeout of 2 seconds is used. This default is subject to change in the future.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NavigationDelayForInitialSiteListDownloadTimeout
- GP name: Set a timeout for delay of tab navigation for the Enterprise Mode Site List
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge

- Path (Recommended): N/A
- Value Name: NavigationDelayForInitialSiteListDownloadTimeout
- Value Type: REG_DWORD

Example value:

```
0x0000000a
```

Back to top

NetworkPredictionOptions

Enable network prediction

Supported versions:

- On Windows and macOS since 77 or later

Description

Enables network prediction and prevents users from changing this setting.

This controls DNS prefetching, TCP and SSL preconnection, and prerendering of web pages.

If you don't configure this policy, network prediction is enabled but the user can change it.

Policy options mapping:

- NetworkPredictionAlways (0) = Predict network actions on any network connection
- NetworkPredictionWifiOnly (1) = Not supported, if this value is used it will be treated as if 'Predict network actions on any network connection' (0) was set
- NetworkPredictionNever (2) = Don't predict network actions on any network connection

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NetworkPredictionOptions
- GP name: Enable network prediction
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: NetworkPredictionOptions
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: NetworkPredictionOptions
- Example value:

```
<integer>2</integer>
```

Back to top

NetworkServiceSandboxEnabled

Enable the network service sandbox

Supported versions:

- On Windows since 102 or later

Description

This policy controls whether or not the network service process runs sandboxed. If this policy is enabled, the network service process will run sandboxed. If this policy is disabled, the network service process will run unsandboxed. This leaves users open to additional security risks related to running the network service unsandboxed. If this policy is not set, the default configuration for the network sandbox will be used. This may vary depending on Microsoft Edge release, currently running field trials, and platform. This policy is intended to give enterprises flexibility to disable the network sandbox if they use third party software that interferes with the network service sandbox.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NetworkServiceSandboxEnabled
- GP name: Enable the network service sandbox
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: NetworkServiceSandboxEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

NonRemovableProfileEnabled

Configure whether a user always has a default profile automatically signed in with their work or school account

Supported versions:

- On Windows since 78 or later

Description

This policy determines if a user can remove the Microsoft Edge profile automatically signed in with a user's work or school account.

If you enable this policy, a non-removable profile will be created with the user's work or school account on Windows. This profile can't be signed out or removed. The profile will be non-removable only if profile is signed-in with either on-premises account or Azure AD account that matches OS sign-in account.

If you disable or don't configure this policy, the profile automatically signed in with a user's work or school account on Windows can be signed out or removed by the user.

If you want to configure browser sign in, use the BrowserSignin policy.

This policy is available only on Windows instances that are joined to a Microsoft Active Directory domain, Windows 10 Pro or Enterprise instances that enrolled for device management.

From Microsoft Edge 89 onwards, if there is an existing on-premises profile with sync disabled and machine is hybrid joined, it will auto-upgrade the on-premises profile to Azure AD profile and make it non-removable instead of creating a new non-removable Azure AD profile.

From Microsoft Edge 93 onwards, if policy ImplicitSignInEnabled is disabled, this policy will not take any effect.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: NonRemovableProfileEnabled
- GP name: Configure whether a user always has a default profile automatically signed in with their work or school account
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: NonRemovableProfileEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

OriginAgentClusterDefaultEnabled

Origin-keyed agent clustering enabled by default

Supported versions:

- On Windows and macOS since 103 or later

Description

The Origin-Agent-Cluster: HTTP header controls whether a document is isolated in an origin-keyed agent cluster

or in a site-keyed agent cluster. This has security implications because an origin-keyed agent cluster allows isolating documents by origin. The consequence of this for developers is that the document.domain accessor can no longer be set when origin-keyed agent clustering is enabled.

If you enable or don't configure this policy, documents without the Origin-Agent-Cluster: header will be assigned to origin-keyed agent clustering by default. On these documents, the document.domain accessor will not be settable.

If you disable this policy, documents without the Origin-Agent-Cluster: header will be assigned to site-keyed agent clusters by default. On these documents, the document.domain accessor will be settable.

See https://go.microsoft.com/fwlink/?linkid=2191896 for additional details.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: OriginAgentClusterDefaultEnabled
- GP name: Origin-keyed agent clustering enabled by default
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: OriginAgentClusterDefaultEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: OriginAgentClusterDefaultEnabled
- Example value:

```
<false/>
```

Back to top

OutlookHubMenuEnabled

Allow users to access the Outlook menu (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 105.

Supported versions:

- On Windows and macOS since 102, until 105

Description

This policy doesn't work because the Outlook menu is now contained within the Edge Sidebar and can be managed using the HubsSidebarEnabled policy.

This policy is used to manage access to the Outlook menu from Microsoft Edge.

If you enable or don't configure this policy, users can access the Outlook menu. If you disable this policy, users can't access the Outlook menu.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: OutlookHubMenuEnabled
- GP name: Allow users to access the Outlook menu (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: OutlookHubMenuEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: OutlookHubMenuEnabled
- Example value:

```
<false/>
```

Back to top

OverrideSecurityRestrictionsOnInsecureOrigin

Control where security restrictions on insecure origins apply

Supported versions:

- On Windows and macOS since 77 or later

Description

Specifies a list of origins (URLs) or hostname patterns (like "*.contoso.com") for which security restrictions on insecure origins don't apply.

This policy lets you specify allowed origins for legacy applications that can't deploy TLS or set up a staging server for internal web development so that developers can test out features requiring secure contexts without having to deploy TLS on the staging server. This policy also prevents the origin from being labeled "Not Secure" in the omnibox.

Setting a list of URLs in this policy has the same effect as setting the command-line flag '--unsafely-treat-insecure-origin-as-secure' to a comma-separated list of the same URLs. If you enable this policy, it overrides the command-line flag.

For more information on secure contexts, see https://www.w3.org/TR/secure-contexts/.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: OverrideSecurityRestrictionsOnInsecureOrigin
- GP name: Control where security restrictions on insecure origins apply
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\OverrideSecurityRestrictionsOnInsecureOrigin
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\OverrideSecurityRestrictionsOnInsecureOrigin\1 =
"http://testserver.contoso.com/"
SOFTWARE\Policies\Microsoft\Edge\OverrideSecurityRestrictionsOnInsecureOrigin\2 = "*.contoso.com"
```

Mac information and settings

- Preference Key Name: OverrideSecurityRestrictionsOnInsecureOrigin
- Example value:

```
<array>
  <string>http://testserver.contoso.com/</string>
  <string>*.contoso.com</string>
</array>
```

Back to top

PDFSecureMode

Secure mode and Certificate-based Digital Signature validation in native PDF reader

Supported versions:

- On Windows and macOS since 100 or later

Description

The policy enables Digital Signature validation for PDF files in a secure environment, which shows the correct validation status of the signatures.

If you enable this policy, PDF files with Certificate-based digital signatures are opened with an option to view and verify the validity of the signatures with high security.

If you disable or don't configure this policy, the capability to view and verify the signature will not be available.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PDFSecureMode
- GP name: Secure mode and Certificate-based Digital Signature validation in native PDF reader
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PDFSecureMode
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: PDFSecureMode
- Example value:

```
<true/>
```

Back to top

PDFXFAEnabled

XFA support in native PDF reader enabled

Supported versions:

- On Windows and macOS since 104 or later

Description

Lets the Microsoft Edge browser enable XFA (XML Forms Architecture) support in the native PDF reader and allows users to open XFA PDF files in the browser.

If you enable this policy, XFA support in the native PDF reader will be enabled.

If you disable or don't configure this policy, Microsoft Edge will not enable XFA support in the native PDF reader.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PDFXFAEnabled
- GP name: XFA support in native PDF reader enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PDFXFAEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: PDFXFAEnabled
- Example value:

```
<true/>
```

Back to top

PaymentMethodQueryEnabled

Allow websites to query for available payment methods

Supported versions:

- On Windows and macOS since 80 or later

Description

Allows you to set whether websites can check if the user has payment methods saved.

If you disable this policy, websites that use PaymentRequest.canMakePayment or PaymentRequest.hasEnrolledInstrument API will be informed that no payment methods are available.

If you enable this policy or don't set this policy, websites can check if the user has payment methods saved.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PaymentMethodQueryEnabled
- GP name: Allow websites to query for available payment methods
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PaymentMethodQueryEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: PaymentMethodQueryEnabled
- Example value:

```
<true/>
```

Back to top

PersonalizationReportingEnabled

Allow personalization of ads, Microsoft Edge, search, news and other Microsoft services by sending browsing history, favorites and collections, usage and other browsing data to Microsoft

Supported versions:

- On Windows and macOS since 80 or later

Description

This policy prevents Microsoft from collecting a user's Microsoft Edge browsing history, favorites and collections, usage, and other browsing data to be used for personalizing advertising, search, news, Microsoft Edge and other Microsoft services.

This setting is not available for child accounts or enterprise accounts.

If you disable this policy, users can't change or override the setting. If this policy is enabled or not configured, Microsoft Edge will default to the user's preference.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PersonalizationReportingEnabled
- GP name: Allow personalization of ads, Microsoft Edge, search, news and other Microsoft services by sending browsing history, favorites and collections, usage and other browsing data to Microsoft
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PersonalizationReportingEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: PersonalizationReportingEnabled
- Example value:

```
<true/>
```

Back to top

PinningWizardAllowed

Allow Pin to taskbar wizard

Supported versions:

- On Windows since 80 or later

Description

Microsoft Edge uses the Pin to taskbar wizard to help users pin suggested sites to the taskbar. The Pin to taskbar wizard feature is enabled by default and accessible to the user through the Settings and more menu.

If you enable this policy or don't configure it, users can call the Pin to taskbar wizard from the Settings and More menu. The wizard can also be called via a protocol launch.

If you disable this policy, the Pin to taskbar wizard is disabled in the menu and cannot be called via a protocol launch.

User settings to enable or disable the Pin to taskbar wizard aren't available.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PinningWizardAllowed
- GP name: Allow Pin to taskbar wizard
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PinningWizardAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

ProactiveAuthEnabled

Enable Proactive Authentication (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 90.

Supported versions:

- On Windows and macOS since 77, until 90

Description

This policy is obsolete because it does not work independently of browser sign in. It does not work in Microsoft Edge after version 90. If you want to configure browser sign in, use the BrowserSignin policy.

Lets you configure whether to turn on Proactive Authentication in Microsoft Edge.

If you enable this policy, Microsoft Edge tries to seamlessly authenticate to websites and services using the account which is signed-in to the browser.

If you disable this policy, Microsoft Edge does not try to authenticate with websites or services using single sign-on (SSO). Authenticated experiences like the Enterprise New Tab Page will not work (e.g. recent and recommended Office documents will not be available).

If you don't configure this policy, Proactive Authentication is turned on.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ProactiveAuthEnabled
- GP name: Enable Proactive Authentication (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ProactiveAuthEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ProactiveAuthEnabled
- Example value:

```
<true/>
```

Back to top

PromotionalTabsEnabled

Enable full-tab promotional content

Supported versions:

- On Windows and macOS since 77 or later

Description

Control the presentation of full-tab promotional or educational content. This setting controls the presentation of welcome pages that help users sign into Microsoft Edge, choose their default browser, or learn about product features.

If you enable this policy (set it true) or don't configure it, Microsoft Edge can show full-tab content to users to provide product information.

If you disable (set to false) this policy, Microsoft Edge can't show full-tab content to users.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PromotionalTabsEnabled
- GP name: Enable full-tab promotional content
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PromotionalTabsEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: PromotionalTabsEnabled
- Example value:

```
<false/>
```

Back to top

PromptForDownloadLocation

Ask where to save downloaded files

Supported versions:

- On Windows and macOS since 77 or later

Description

Set whether to ask where to save a file before downloading it.

If you enable this policy, the user is asked where to save each file before downloading; if you don't configure it, files are saved automatically to the default location, without asking the user.

If you don't configure this policy, the user will be able to change this setting.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PromptForDownloadLocation
- GP name: Ask where to save downloaded files
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PromptForDownloadLocation
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: PromptForDownloadLocation
- Example value:

```
<false/>
```

Back to top

PromptOnMultipleMatchingCertificates

Prompt the user to select a certificate when multiple certificates match

Supported versions:

- On Windows and macOS since 100 or later

Description

This policy controls whether the user is prompted to select a client certificate when more than one certificate matches AutoSelectCertificateForUrls. If this policy is set to True, the user is prompted to select a client certificate whenever the auto-selection policy matches multiple certificates. If this policy is set to False or not set, the user may only be prompted when no certificate matches the auto-selection.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: PromptOnMultipleMatchingCertificates
- GP name: Prompt the user to select a certificate when multiple certificates match
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: PromptOnMultipleMatchingCertificates
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: PromptOnMultipleMatchingCertificates
- Example value:

```
<true/>
```

Back to top

QuicAllowed

Allow QUIC protocol

Supported versions:

- On Windows and macOS since 77 or later

Description

Allows use of the QUIC protocol in Microsoft Edge.

If you enable this policy or don't configure it, the QUIC protocol is allowed.

If you disable this policy, the QUIC protocol is blocked.

QUIC is a transport layer network protocol that can improve performance of web applications that currently use TCP.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: QuicAllowed
- GP name: Allow QUIC protocol
- GP path (Mandatory): Administrative Templates/Microsoft Edge/

- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: QuicAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: QuicAllowed
- Example value:

```
<true/>
```

Back to top

QuickSearchShowMiniMenu

Enables Microsoft Edge mini menu

Supported versions:

- On Windows and macOS since 104 or later

Description

Enables Microsoft Edge mini menu on websites and PDFs. The mini menu is triggered on text selection and has basic actions like copy and smart actions like definitions.

If you enable or don't config this policy, selecting text on websites and PDFs will show the Microsoft Edge mini menu.

If you disable this policy, the Microsoft Edge mini menu will not be shown when text on websites and PDFs is selected.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: QuickSearchShowMiniMenu
- GP name: Enables Microsoft Edge mini menu
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: QuickSearchShowMiniMenu

- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: QuickSearchShowMiniMenu
- Example value:

```
<true/>
```

Back to top

QuickViewOfficeFilesEnabled

Manage QuickView Office files capability in Microsoft Edge

Supported versions:

- On Windows and macOS since 90 or later

Description

Allows you to set whether users can view publicly accessible Office files on the web that aren't on OneDrive or SharePoint. (For example: Word documents, PowerPoint presentations, and Excel spreadsheets)

If you enable or don't configure this policy, these files can be viewed in Microsoft Edge using Office Viewer instead of downloading the files.

If you disable this policy, these files will be downloaded to be viewed.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: QuickViewOfficeFilesEnabled
- GP name: Manage QuickView Office files capability in Microsoft Edge
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: QuickViewOfficeFilesEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: QuickViewOfficeFilesEnabled

- Example value:

```
<true/>
```

Back to top

RedirectSitesFromInternetExplorerPreventBHOInstall

Prevent install of the BHO to redirect incompatible sites from Internet Explorer to Microsoft Edge

Supported versions:

- On Windows since 87 or later

Description

This setting lets you specify whether to block the install of the Browser Helper Object (BHO) that enables redirecting incompatible sites from Internet Explorer to Microsoft Edge for sites that require a modern browser.

If you enable this policy, the BHO will not be installed. If it is already installed it will be uninstalled on the next Microsoft Edge update.

If this policy is not configured or is disabled, the BHO will be installed.

The BHO is required for incompatible site redirection to occur, however whether redirection occurs or not is also controlled by RedirectSitesFromInternetExplorerRedirectMode.

For more information about this policy see https://go.microsoft.com/fwlink/?linkid=2141715

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: RedirectSitesFromInternetExplorerPreventBHOInstall
- GP name: Prevent install of the BHO to redirect incompatible sites from Internet Explorer to Microsoft Edge
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: RedirectSitesFromInternetExplorerPreventBHOInstall
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

RedirectSitesFromInternetExplorerRedirectMode

Redirect incompatible sites from Internet Explorer to Microsoft Edge

Supported versions:

- On Windows since 87 or later

Description

This setting lets you specify whether Internet Explorer will redirect navigations to sites that require a modern browser to Microsoft Edge. If you set this policy to 'Disable' ('Prevent redirection', value 0), Internet Explorer will not redirect any traffic to Microsoft Edge.

If you set this policy to 'Sitelist', starting with Microsoft Edge major release 87 , Internet Explorer (IE) will redirect sites that require a modern browser to Microsoft Edge. (Note: The Sitelist setting is 'Redirect sites based on the incompatible sites sitelist', value 1).

When a site is redirected from Internet Explorer to Microsoft Edge, the Internet Explorer tab that started loading the site is closed if it had no prior content. Otherwise, the user is taken to a Microsoft help page that explains why the site was redirected to Microsoft Edge. When Microsoft Edge is launched to load an IE site, an information bar explains that the site works best in a modern browser.

If you want to redirect all navigations, you can configure the Disable Internet Explorer 11 policy, which redirects all navigations from IE11 to Microsoft Edge. It also hides the IE11 app icon from the user after the first launch.

If don't configure this policy:

- Starting with Microsoft Edge major release 87, you will have the same experience as setting the policy to 'Sitelist': Internet Explorer will redirect sites that require a modern browser to Microsoft Edge.
- In the future, the default for your organization might change to automatically redirect all navigations. If you don't want automatic redirection, set this policy to 'Disable' or 'Sitelist'.

For more information about this policy see https://go.microsoft.com/fwlink/?linkid=2141715

Policy options mapping:

- Disable (0) = Prevent redirection
- Sitelist (1) = Redirect sites based on the incompatible sites sitelist

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: RedirectSitesFromInternetExplorerRedirectMode
- GP name: Redirect incompatible sites from Internet Explorer to Microsoft Edge
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: RedirectSitesFromInternetExplorerRedirectMode
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

RelatedMatchesCloudServiceEnabled

Configure Related Matches in Find on Page

Supported versions:

- On Windows and macOS since 99 or later

Description

Specifies how the user receives related matches in Find on Page, which provides spellcheck, synonyms, and Q&A results in Microsoft Edge.

If you enable or don't configure this policy, users can receive related matches in Find on Page on all sites. The results are processed in a cloud service.

If you disable this policy, users can receive related matches in Find on Page on limited sites. The results are processed on the user's device.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: RelatedMatchesCloudServiceEnabled
- GP name: Configure Related Matches in Find on Page
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: RelatedMatchesCloudServiceEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: RelatedMatchesCloudServiceEnabled
- Example value:

```
<true/>
```

Back to top

RelaunchNotification

Notify a user that a browser restart is recommended or required for pending updates

Supported versions:

- On Windows and macOS since 77 or later

Description

Notify users that they need to restart Microsoft Edge to apply a pending update.

If you don't configure this policy, Microsoft Edge adds a recycle icon at the far right of the top menu bar to prompt users to restart the browser to apply the update.

If you enable this policy and set it to 'Recommended', a recurring warning prompts users that a restart is recommended. Users can dismiss this warning and defer the restart.

If you set the policy to 'Required', a recurring warning prompts users that the browser will be restarted automatically as soon as a notification period passes. The default period is seven days. You can configure this period with the RelaunchNotificationPeriod policy.

The user's session is restored when the browser restarts.

Policy options mapping:

- Recommended (1) = Recommended - Show a recurring prompt to the user indicating that a restart is recommended
- Required (2) = Required - Show a recurring prompt to the user indicating that a restart is required

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: RelaunchNotification
- GP name: Notify a user that a browser restart is recommended or required for pending updates
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: RelaunchNotification
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: RelaunchNotification
- Example value:

```
<integer>1</integer>
```

Back to top

RelaunchNotificationPeriod

Set the time period for update notifications

Supported versions:

- On Windows and macOS since 77 or later

Description

Allows you to set the time period, in milliseconds, over which users are notified that Microsoft Edge must be relaunched to apply a pending update.

Over this time period, the user will be repeatedly informed of the need for an update. In Microsoft Edge the app menu changes to indicate that a relaunch is needed once one third of the notification period passes. This notification changes color once two thirds of the notification period passes, and again once the full notification period has passed. The additional notifications enabled by the RelaunchNotification policy follow this same schedule.

If not set, the default period of 604800000 milliseconds (one week) is used.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: RelaunchNotificationPeriod
- GP name: Set the time period for update notifications
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: RelaunchNotificationPeriod
- Value Type: REG_DWORD

Example value:

```
0x240c8400
```

Mac information and settings

- Preference Key Name: RelaunchNotificationPeriod
- Example value:

```
<integer>604800000</integer>
```

Back to top

RelaunchWindow

Set the time interval for relaunch

Supported versions:

- On Windows and macOS since 93 or later

Description

Specifies a target time window for the end of the relaunch notification period.

Users are notified of the need for a browser relaunch or device restart based on the RelaunchNotification and RelaunchNotificationPeriod policy settings. Browsers and devices are forcibly restarted at the end of the notification period when the RelaunchNotification policy is set to 'Required'. This RelaunchWindow policy can be used to defer the end of the notification period so that it falls within a specific time window.

If you don't configure this policy, the default target time window is the whole day (i.e., the end of the notification period is never deferred).

Note: Though the policy can accept multiple items in entries, all but the first item are ignored. Warning: Setting this policy may delay application of software updates.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Dictionary

Windows information and settings

Group Policy (ADMX) info

- GP unique name: RelaunchWindow
- GP name: Set the time interval for relaunch
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: RelaunchWindow
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\RelaunchWindow = {
  "entries": [
    {
      "duration_mins": 240,
      "start": {
        "hour": 2,
        "minute": 15
      }
    }
  ]
}
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\RelaunchWindow = {"entries": [{"duration_mins": 240, "start": {"hour": 2,
"minute": 15}}]}
```

Mac information and settings

- Preference Key Name: RelaunchWindow
- Example value:

```
<key>RelaunchWindow</key>
<dict>
  <key>entries</key>
  <array>
    <dict>
      <key>duration_mins</key>
      <integer>240</integer>
      <key>start</key>
      <dict>
        <key>hour</key>
        <integer>2</integer>
        <key>minute</key>
        <integer>15</integer>
      </dict>
    </dict>
  </array>
</dict>
```

Back to top

RemoteDebuggingAllowed

Allow remote debugging

Supported versions:

- On Windows and macOS since 93 or later

Description

Controls whether users may use remote debugging.

If you enable or don't configure this policy, users may use remote debugging by specifying --remote-debug-port and --remote-debugging-pipe command line switches.

If you disable this policy, users are not allowed to use remote debugging.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: RemoteDebuggingAllowed
- GP name: Allow remote debugging
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge

- Path (Recommended): N/A
- Value Name: RemoteDebuggingAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: RemoteDebuggingAllowed
- Example value:

```
<true/>
```

Back to top

RendererAppContainerEnabled

Enable renderer in app container

Supported versions:

- On Windows since 96 or later

Description

Launches Renderer processes into an App Container for additional security benefits.

If you don't configure this policy, Microsoft Edge will launch the renderer process in an app container in a future update.

If you enable this policy, Microsoft Edge will launch the renderer process in an app container.

If you disable this policy, Microsoft Edge will not launch the renderer process in an app container.

Only turn off the policy if there are compatibility issues with third-party software that must run inside Microsoft Edge's renderer processes.

This policy is only supported on Windows 10 devices.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: RendererAppContainerEnabled
- GP name: Enable renderer in app container
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: RendererAppContainerEnabled

- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

RendererCodeIntegrityEnabled

Enable renderer code integrity

Supported versions:

- On Windows since 78 or later

Description

Setting the policy to Enabled or leaving it unset turns Renderer Code Integrity on. Setting the policy to Disabled has a detrimental effect on Microsoft Edge's security and stability as unknown and potentially hostile code can load inside Microsoft Edge's renderer processes. Only turn off the policy if there are compatibility issues with third-party software that must run inside Microsoft Edge's renderer processes.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: RendererCodeIntegrityEnabled
- GP name: Enable renderer code integrity
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: RendererCodeIntegrityEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

RequireOnlineRevocationChecksForLocalAnchors

Specify if online OCSP/CRL checks are required for local trust anchors

Supported versions:

- On Windows since 77 or later

Description

Control whether online revocation checks (OCSP/CRL checks) are required. If Microsoft Edge can't get revocation status information, these certificates are treated as revoked ("hard-fail").

If you enable this policy, Microsoft Edge always performs revocation checking for server certificates that

successfully validate and are signed by locally-installed CA certificates.

If you don't configure or disable this policy, then Microsoft Edge uses the existing online revocation checking settings.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: RequireOnlineRevocationChecksForLocalAnchors
- GP name: Specify if online OCSP/CRL checks are required for local trust anchors
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: RequireOnlineRevocationChecksForLocalAnchors
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

ResolveNavigationErrorsUseWebService

Enable resolution of navigation errors using a web service

Supported versions:

- On Windows and macOS since 77 or later

Description

Allow Microsoft Edge to issue a dataless connection to a web service to probe networks for connectivity in cases like hotel and airport Wi-Fi.

If you enable this policy, a web service is used for network connectivity tests.

If you disable this policy, Microsoft Edge uses native APIs to try to resolve network connectivity and navigation issues.

Note: Except on Windows 8 and later versions of Windows, Microsoft Edge *always* uses native APIs to resolve connectivity issues.

If you don't configure this policy, Microsoft Edge respects the user preference that's set under Services at edge://settings/privacy. Specifically, there's a **Use a web service to help resolve navigation errors** toggle, which the user can switch on or off. Be aware that if you have enabled this policy (ResolveNavigationErrorsUseWebService), the **Use a web service to help resolve navigation errors** setting is turned on, but the user can't change the setting by using the toggle. If you have disabled this policy, the **Use a web service to help resolve navigation errors** setting is turned off, and the user can't change the setting by using the toggle.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ResolveNavigationErrorsUseWebService
- GP name: Enable resolution of navigation errors using a web service
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ResolveNavigationErrorsUseWebService
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ResolveNavigationErrorsUseWebService
- Example value:

```
<true/>
```

Back to top

RestrictSigninToPattern

Restrict which accounts can be used to sign in to Microsoft Edge

Supported versions:

- On Windows and macOS since 77 or later

Description

Determines which accounts can be used to sign in to the Microsoft Edge account that's chosen during the Sync opt-in flow.

You can configure this policy to match multiple accounts using a Perl style regular expression for the pattern. If a user tries to sign in to the browser with an account whose username doesn't match this pattern, they are blocked and will get the appropriate error message. Note that pattern matches are case sensitive. For more information about the regular expression rules that are used, refer to https://go.microsoft.com/fwlink/p/?linkid=2133903.

If you don't configure this policy or leave it blank, users can use any account to sign in to Microsoft Edge.

Note that signed-in profiles with a username that doesn't match this pattern will be signed out after this policy is enabled.

Supported features:

- Can be mandatory: Yes

- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: RestrictSigninToPattern
- GP name: Restrict which accounts can be used to sign in to Microsoft Edge
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: RestrictSigninToPattern
- Value Type: REG_SZ

Example value:

```
".*@contoso.com"
```

Mac information and settings

- Preference Key Name: RestrictSigninToPattern
- Example value:

```
<string>.*@contoso.com</string>
```

Back to top

RoamingProfileLocation

Set the roaming profile directory

Supported versions:

- On Windows since 85 or later

Description

Configures the directory to use to store the roaming copy of profiles.

If you enable this policy, Microsoft Edge uses the provided directory to store a roaming copy of the profiles, as long as you've also enabled the RoamingProfileSupportEnabled policy. If you disable the RoamingProfileSupportEnabled policy or don't configure it, the value stored in this policy isn't used.

See https://go.microsoft.com/fwlink/?linkid=2095041 for a list of variables you can use.

If you don't configure this policy, the default roaming profile path is used.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: RoamingProfileLocation
- GP name: Set the roaming profile directory
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: RoamingProfileLocation
- Value Type: REG_SZ

Example value:

```
"${roaming_app_data}\\edge-profile"
```

Back to top

RoamingProfileSupportEnabled

Enable using roaming copies for Microsoft Edge profile data

Supported versions:

- On Windows since 85 or later

Description

Enable this policy to use roaming profiles on Windows. The settings stored in Microsoft Edge profiles (favorites and preferences) are also saved to a file stored in the Roaming user profile folder (or the location specified by the administrator through the RoamingProfileLocation policy).

If you disable this policy or don't configure it, only the regular local profiles are used.

The SyncDisabled only disables cloud synchronization and has no impact on this policy.

See https://go.microsoft.com/fwlink/?linkid=2150058 for more information on using roaming user profiles.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: RoamingProfileSupportEnabled
- GP name: Enable using roaming copies for Microsoft Edge profile data
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: RoamingProfileSupportEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

RunAllFlashInAllowMode

Extend Adobe Flash content setting to all content (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 88.

Supported versions:

- On Windows and macOS since 77, until 88

Description

This policy doesn't work because Flash is no longer supported by Microsoft Edge.

If you enable this policy, all Adobe Flash content embedded in websites that are set to allow Adobe Flash in the content settings -- either by the user or by enterprise policy -- will run. This includes content from other origins and/or small content.

To control which websites are allowed to run Adobe Flash, see the specifications in the DefaultPluginsSetting, PluginsAllowedForUrls, and PluginsBlockedForUrls policies.

If you disable this policy or don't configure it, Adobe Flash content from other origins (from sites that aren't specified in the three policies mentioned immediately above) or small content might be blocked.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: RunAllFlashInAllowMode
- GP name: Extend Adobe Flash content setting to all content (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: RunAllFlashInAllowMode
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: RunAllFlashInAllowMode
- Example value:

```
<true/>
```

Back to top

SSLErrorOverrideAllowed

Allow users to proceed from the HTTPS warning page

Supported versions:

- On Windows and macOS since 77 or later

Description

Microsoft Edge shows a warning page when users visit sites that have SSL errors.

If you enable or don't configure (default) this policy, users can click through these warning pages.

If you disable this policy, users are blocked from clicking through any warning page.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SSLErrorOverrideAllowed
- GP name: Allow users to proceed from the HTTPS warning page
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: SSLErrorOverrideAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: SSLErrorOverrideAllowed
- Example value:

```
<true/>
```

Back to top

SSLErrorOverrideAllowedForOrigins

Allow users to proceed from the HTTPS warning page for specific origins

Supported versions:

- On Windows and macOS since 90 or later

Description

Microsoft Edge shows a warning page when users visit sites that have SSL errors.

If you enable or don't configure the SSLErrorOverrideAllowed policy, this policy does nothing.

If you disable the SSLErrorOverrideAllowed policy, configuring this policy lets you configure a list of origin patterns for sites where users can continue to click through SSL error pages. Users can't click through SSL error pages on origins that are not on this list.

If you don't configure this policy, the SSLErrorOverrideAllowed policy applies for all sites.

For detailed information about valid origin patterns, see https://go.microsoft.com/fwlink/?linkid=2095322. * is not an accepted value for this policy. This policy only matches based on origin, so any path or query in the URL pattern is ignored.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SSLErrorOverrideAllowedForOrigins
- GP name: Allow users to proceed from the HTTPS warning page for specific origins
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\SSLErrorOverrideAllowedForOrigins
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\SSLErrorOverrideAllowedForOrigins\1 = "https://www.example.com"
SOFTWARE\Policies\Microsoft\Edge\SSLErrorOverrideAllowedForOrigins\2 = "[*.]example.edu"
```

Mac information and settings

- Preference Key Name: SSLErrorOverrideAllowedForOrigins
- Example value:

```
<array>
  <string>https://www.example.com</string>
  <string>[*.]example.edu</string>
</array>
```

Back to top

SSLVersionMin

Minimum TLS version enabled

Supported versions:

- On Windows and macOS since 77 or later

Description

Sets the minimum supported version of TLS.

If you set this policy to 'tls1.2', Microsoft Edge will show an error for TLS 1.0 and TLS 1.1 and the user will not be able to bypass the error.

If you don't configure this policy, Microsoft Edge will still show an error for TLS 1.0 and TLS 1.1 but the user will be able to bypass it.

Support for suppressing the TLS 1.0/1.1 warning was removed from Microsoft Edge starting in version 91. The 'tls1' and 'tls1.1' values are no longer supported.

Policy options mapping:

- TLSv1 (tls1) = TLS 1.0
- TLSv1.1 (tls1.1) = TLS 1.1
- TLSv1.2 (tls1.2) = TLS 1.2

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SSLVersionMin
- GP name: Minimum TLS version enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: SSLVersionMin
- Value Type: REG_SZ

Example value:

```
"tls1"
```

Mac information and settings

- Preference Key Name: SSLVersionMin
- Example value:

```
<string>tls1</string>
```

Back to top

SandboxExternalProtocolBlocked

Allow Microsoft Edge to block navigations to external protocols in a sandboxed iframe

Supported versions:

- On Windows and macOS since 99 or later

Description

Microsoft Edge will block navigations to external protocols inside a sandboxed iframe.

If you enable or don't configure this policy, Microsoft Edge will block those navigations.

If you disable this policy, Microsoft Edge will not block those navigations.

This can be used by administrators who need more time to update their internal website affected by this new restriction. This Enterprise policy is temporary; it's intended to be removed after Microsoft Edge version 117.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SandboxExternalProtocolBlocked
- GP name: Allow Microsoft Edge to block navigations to external protocols in a sandboxed iframe
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: SandboxExternalProtocolBlocked
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: SandboxExternalProtocolBlocked
- Example value:

```
<true/>
```

Back to top

SaveCookiesOnExit

Save cookies when Microsoft Edge closes

Supported versions:

- On Windows and macOS since 86 or later

Description

When this policy is enabled, the specified set of cookies is exempt from deletion when the browser closes. This policy is only effective when:

- The 'Cookies and other site data' toggle is configured in Settings/Privacy and services/Clear browsing data

on close or

- The policy ClearBrowsingDataOnExit is enabled or
- The policy DefaultCookiesSetting is set to 'Keep cookies for the duration of the session'.

You can define a list of sites, based on URL patterns, that will have their cookies preserved across sessions.

Note: Users can still edit the cookie site list to add or remove URLs. However, they can't remove URLs that have been added by an Admin.

If you enable this policy, the list of cookies won't be cleared when the browser closes.

If you disable or don't configure this policy, the user's personal configuration is used.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SaveCookiesOnExit
- GP name: Save cookies when Microsoft Edge closes
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\SaveCookiesOnExit
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\SaveCookiesOnExit\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\SaveCookiesOnExit\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: SaveCookiesOnExit
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

SavingBrowserHistoryDisabled

Disable saving browser history

Supported versions:

- On Windows and macOS since 77 or later

Description

Disables saving browser history and prevents users from changing this setting.

If you enable this policy, browsing history isn't saved. This also disables tab syncing.

If you disable this policy or don't configure it, browsing history is saved.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SavingBrowserHistoryDisabled
- GP name: Disable saving browser history
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: SavingBrowserHistoryDisabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: SavingBrowserHistoryDisabled
- Example value:

```
<true/>
```

Back to top

ScreenCaptureAllowed

Allow or deny screen capture

Supported versions:

- On Windows and macOS since 83 or later

Description

If you enable this policy, or don't configure this policy, a web page can use screen-share APIs (for example, getDisplayMedia() or the Desktop Capture extension API) for a screen capture. If you disable this policy, calls to screen-share APIs will fail. For example, if you're using a web-based online meeting, video or screen sharing will not work. However, this policy is not considered (and a site will be allowed to use screen-share APIs) if the site matches an origin pattern in any of the following policies: ScreenCaptureAllowedByOrigins, WindowCaptureAllowedByOrigins, TabCaptureAllowedByOrigins, SameOriginTabCaptureAllowedByOrigins.

Supported features:

- Can be mandatory: Yes

- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ScreenCaptureAllowed
- GP name: Allow or deny screen capture
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ScreenCaptureAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: ScreenCaptureAllowed
- Example value:

```
<false/>
```

Back to top

ScrollToTextFragmentEnabled

Enable scrolling to text specified in URL fragments

Supported versions:

- On Windows and macOS since 83 or later

Description

This feature lets hyperlink and address bar URL navigations target specific text on a web page, which will be scrolled to after the web page finishes loading.

If you enable or don't configure this policy, web page scrolling to specific text fragments via a URL will be enabled.

If you disable this policy, web page scrolling to specific text fragments via a URL will be disabled.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ScrollToTextFragmentEnabled

- GP name: Enable scrolling to text specified in URL fragments
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ScrollToTextFragmentEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: ScrollToTextFragmentEnabled
- Example value:

```
<false/>
```

Back to top

SearchSuggestEnabled

Enable search suggestions

Supported versions:

- On Windows and macOS since 77 or later

Description

Enables web search suggestions in Microsoft Edge's Address Bar and Auto-Suggest List and prevents users from changing this policy.

If you enable this policy, web search suggestions are used.

If you disable this policy, web search suggestions are never used, however local history and local favorites suggestions still appear. If you disable this policy, neither the typed characters, nor the URLs visited will be included in telemetry to Microsoft.

If this policy is left not set, search suggestions are enabled but the user can change that.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SearchSuggestEnabled
- GP name: Enable search suggestions
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: SearchSuggestEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: SearchSuggestEnabled
- Example value:

```
<true/>
```

Back to top

SecurityKeyPermitAttestation

Websites or domains that don't need permission to use direct Security Key attestation

Supported versions:

- On Windows and macOS since 77 or later

Description

Specifies websites and domains that don't need explicit user permission when attestation certificates from security keys are requested. Additionally, a signal is sent to the security key indicating that it can use individual attestation. Without this, users are prompted each time a site requests attestation of security keys.

Sites (like https://contoso.com/some/path) only match as U2F appIDs. Domains (like contoso.com) only match as webauthn RP IDs. To cover both U2F and webauthn APIs for a given site, you need to list both the appID URL and domain.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SecurityKeyPermitAttestation
- GP name: Websites or domains that don't need permission to use direct Security Key attestation
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\SecurityKeyPermitAttestation
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\SecurityKeyPermitAttestation\1 = "https://contoso.com"
```

Mac information and settings

- Preference Key Name: SecurityKeyPermitAttestation
- Example value:

```
<array>
  <string>https://contoso.com</string>
</array>
```

Back to top

SendIntranetToInternetExplorer

Send all intranet sites to Internet Explorer

Supported versions:

- On Windows since 77 or later

Description

For guidance about configuring the optimal experience for Internet Explorer mode see https://go.microsoft.com/fwlink/?linkid=2094210

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SendIntranetToInternetExplorer
- GP name: Send all intranet sites to Internet Explorer
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: SendIntranetToInternetExplorer
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

SendSiteInfoToImproveServices

Send site information to improve Microsoft services (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 88.

Supported versions:

- On Windows and macOS since 77, until 88

Description

This policy is no longer supported. It is replaced by DiagnosticData (for Windows 7, Windows 8, and macOS) and Allow Telemetry on Win 10 (https://go.microsoft.com/fwlink/?linkid=2099569).

This policy enables sending info about websites visited in Microsoft Edge to Microsoft to improve services like search.

Enable this policy to send info about websites visited in Microsoft Edge to Microsoft. Disable this policy to not send info about websites visited in Microsoft Edge to Microsoft. In both cases, users can't change or override the setting.

On Windows 10, if you don't configure this policy, Microsoft Edge will default to the Windows diagnostic data setting. If this policy is enabled Microsoft Edge will only send info about websites visited in Microsoft Edge if the Windows Diagnostic data setting is set to Full. If this policy is disabled Microsoft Edge will not send info about websites visited. Learn more about Windows Diagnostic data settings: https://go.microsoft.com/fwlink/?linkid=2099569

On Windows 7, windows 8, and macOS this policy controls sending info about websites visited. If you don't configure this policy, Microsoft Edge will default to the user's preference.

To enable this policy, MetricsReportingEnabled must be set to Enabled. If SendSiteInfoToImproveServices or MetricsReportingEnabled is Not Configured or Disabled, this data will not be sent to Microsoft.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SendSiteInfoToImproveServices
- GP name: Send site information to improve Microsoft services (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: SendSiteInfoToImproveServices
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: SendSiteInfoToImproveServices
- Example value:

```
<false/>
```

Back to top

SensorsAllowedForUrls

Allow access to sensors on specific sites

Supported versions:

- On Windows and macOS since 86 or later

Description

Define a list of sites, based on URL patterns, that can access and use sensors such as motion and light sensors.

If you don't configure this policy, the global default value from the DefaultSensorsSetting policy (if set) or the user's personal configuration is used for all sites.

For URL patterns that don't match this policy, the following order of precedence is used: The SensorsBlockedForUrls policy (if there is a match), the DefaultSensorsSetting policy (if set), or the user's personal settings.

The URL patterns defined in this policy can't conflict with those configured in the SensorsBlockedForUrls policy. You can't allow and block a URL.

For detailed information about valid URL patterns, please see https://go.microsoft.com/fwlink/?linkid=2095322.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SensorsAllowedForUrls
- GP name: Allow access to sensors on specific sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\SensorsAllowedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\SensorsAllowedForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\SensorsAllowedForUrls\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: SensorsAllowedForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

SensorsBlockedForUrls

Block access to sensors on specific sites

Supported versions:

- On Windows and macOS since 86 or later

Description

Define a list of sites, based on URL patterns, that can't access sensors such as motion and light sensors.

If you don't configure this policy, the global default value from the DefaultSensorsSetting policy (if set) or the user's personal configuration is used for all sites.

For URL patterns that don't match this policy, the following order of precedence is used: The SensorsAllowedForUrls policy (if there is a match), the DefaultSensorsSetting policy (if set), or the user's personal settings.

The URL patterns defined in this policy can't conflict with those configured in the SensorsAllowedForUrls policy. You can't allow and block a URL.

For detailed information about valid URL patterns, please see https://go.microsoft.com/fwlink/?linkid=2095322.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SensorsBlockedForUrls
- GP name: Block access to sensors on specific sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\SensorsBlockedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\SensorsBlockedForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\SensorsBlockedForUrls\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: SensorsBlockedForUrls

- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

SerialAskForUrls

Allow the Serial API on specific sites

Supported versions:

- On Windows and macOS since 86 or later

Description

Define a list of sites, based on URL patterns, that can ask the user for access to a serial port.

If you don't configure this policy, the global default value from the DefaultSerialGuardSetting policy (if set) or the user's personal configuration is used for all sites.

For URL patterns that don't match this policy, the following order of precedence is used: The SerialBlockedForUrls policy (if there is a match), the DefaultSerialGuardSetting policy (if set), or the user's personal settings.

The URL patterns defined in this policy can't conflict with those configured in the SerialBlockedForUrls policy. You can't allow and block a URL.

For detailed information about valid url patterns, please see https://go.microsoft.com/fwlink/?linkid=2095322.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SerialAskForUrls
- GP name: Allow the Serial API on specific sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\SerialAskForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\SerialAskForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\SerialAskForUrls\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: SerialAskForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

SerialBlockedForUrls

Block the Serial API on specific sites

Supported versions:

- On Windows and macOS since 86 or later

Description

Define a list of sites, based on URL patterns, that can't ask the user to grant them access to a serial port.

If you don't configure this policy, the global default value from the DefaultSerialGuardSetting policy (if set) or the user's personal configuration is used for all sites.

For URL patterns that don't match this policy, the following order of precedence is used: The SerialAskForUrls policy (if there is a match), the DefaultSerialGuardSetting policy (if set), or the user's personal settings.

The URL patterns in this policy can't conflict with those configured in the SerialAskForUrls policy. You can't allow and block a URL.

For detailed information about valid URL patterns, see https://go.microsoft.com/fwlink/?linkid=2095322.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SerialBlockedForUrls
- GP name: Block the Serial API on specific sites
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\SerialBlockedForUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\SerialBlockedForUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\SerialBlockedForUrls\2 = "[*.]contoso.edu"
```

Mac information and settings

- Preference Key Name: SerialBlockedForUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>[*.]contoso.edu</string>
</array>
```

Back to top

SetTimeoutWithout1MsClampEnabled

Control Javascript setTimeout() function minimum timeout (deprecated)

> DEPRECATED: This policy is deprecated. It is currently supported but will become obsolete in a future release.

Supported versions:

- On Windows and macOS since 101 or later

Description

When the policy is set to Enabled, the Javascript setTimeout() with a timeout of 0ms will no longer be fixed to 1ms to schedule timer-based callbacks. When the policy is set to Disabled, the Javascript setTimeout() with a timeout of 0ms will be fixed to 1ms to schedule timer-based callbacks. When the policy is unset, use the browser's default behavior for setTimeout() function.

This is a web standards compliancy feature, but it may change task ordering on a web page, leading to unexpected behavior on sites that are dependent on a certain ordering. It also may affect sites with a lot of setTimeout()s with a timeout of 0ms usage. For example, increasing CPU load.

For users where this policy is unset, Microsoft Edge Stable will roll out the change gradually on the stable channel.

This is a temporary policy that is planned to be removed in Microsoft Edge Stable 105. This deadline may be extended if there is a need for enterprises.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SetTimeoutWithout1MsClampEnabled
- GP name: Control Javascript setTimeout() function minimum timeout (deprecated)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: SetTimeoutWithout1MsClampEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: SetTimeoutWithout1MsClampEnabled
- Example value:

```
<true/>
```

Back to top

ShadowStackCrashRollbackBehavior

Configure ShadowStack crash rollback behavior (deprecated)

> DEPRECATED: This policy is deprecated. It is currently supported but will become obsolete in a future release.

Supported versions:

- On Windows since 95 or later

Description

This policy is deprecated because it's intended to serve only as a short-term mechanism to give enterprises more time to update their environments and report issues if they are found to be incompatible with Hardware-enforced Stack Protection. It won't work in Microsoft Edge as soon as version 109.

Microsoft Edge includes a Hardware-enforced Stack Protection security feature. This feature may result in the browser crashing unexpectedly in cases that do not represent an attempt to compromise the browser's security.

Using this policy, you may control the behavior of the Hardware-enforced Stack Protection feature after a crash triggered by this feature is encountered.

Set this policy to 'Disable' to disable the feature.

Set this policy to 'DisableUntilUpdate' to disable the feature until Microsoft Edge updates next time.

Set this policy to 'Enable' to keep the feature enabled.

Policy options mapping:

- Disable (0) = Disable Hardware-enforced Stack Protection
- DisableUntilUpdate (1) = Disable Hardware-enforced Stack Protection until the next Microsoft Edge update
- Enable (2) = Enable Hardware-enforced Stack Protection

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ShadowStackCrashRollbackBehavior
- GP name: Configure ShadowStack crash rollback behavior (deprecated)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ShadowStackCrashRollbackBehavior
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

SharedArrayBufferUnrestrictedAccessAllowed

Specifies whether SharedArrayBuffers can be used in a non cross-origin-isolated context

Supported versions:

- On Windows and macOS since 92 or later

Description

Specifies whether SharedArrayBuffers can be used in a non cross-origin-isolated context. A SharedArrayBuffer is a binary data buffer that can be used to create views on shared memory. SharedArrayBuffers have a memory access vulnerability in several popular CPUs.

If you enable this policy, sites are allowed to use SharedArrayBuffers with no restrictions.

If you disable or don't configure this policy, sites are allowed to use SharedArrayBuffers only when cross-origin isolated.

Microsoft Edge will require cross-origin isolation when using SharedArrayBuffers from Microsoft Edge 91 onward for Web Compatibility reasons.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SharedArrayBufferUnrestrictedAccessAllowed
- GP name: Specifies whether SharedArrayBuffers can be used in a non cross-origin-isolated context
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: SharedArrayBufferUnrestrictedAccessAllowed

- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: SharedArrayBufferUnrestrictedAccessAllowed
- Example value:

```
<true/>
```

Back to top

SharedLinksEnabled

Show links shared from Microsoft 365 apps in History

Supported versions:

- On Windows and macOS since 96 or later

Description

Allows Microsoft Edge to display links recently shared by or shared with the user from Microsoft 365 apps in History.

If you enable or don't configure this policy, Microsoft Edge displays links recently shared by or shared with the user from Microsoft 365 apps in History.

If you disable this policy, Microsoft Edge does not display links recently shared by or shared with the user from Microsoft 365 apps in History. The control in Microsoft Edge settings is disabled and set to off.

This policy only applies for Microsoft Edge local user profiles and profiles signed in using Azure Active Directory.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SharedLinksEnabled
- GP name: Show links shared from Microsoft 365 apps in History
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: SharedLinksEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: SharedLinksEnabled
- Example value:

```
<true/>
```

Back to top

ShowMicrosoftRewards

Show Microsoft Rewards experiences

Supported versions:

- On Windows and macOS since 88 or later

Description

Show Microsoft Rewards experience and notifications. If you enable this policy:

- Microsoft account users (excludes Azure AD accounts) in search, new tab page, and earn markets will see the Microsoft Rewards experience in their Microsoft Edge user profile.
- The setting to enable Microsoft Rewards in Microsoft Edge settings will be enabled and toggled on.

If you disable this policy:

- Microsoft account users (excludes Azure AD accounts) in search, new tab page, and earn markets will not see the Microsoft Rewards experience in their Microsoft Edge user profile.
- The setting to enable Microsoft Rewards in Microsoft Edge settings will be disabled and toggled off.

If you don't configure this policy:

- Microsoft account users (excludes Azure AD accounts) in search, new tab page, and earn markets will see the Microsoft Rewards experience in their Microsoft Edge user profile.
- The setting to enable Microsoft Rewards in Microsoft Edge settings will be enabled and toggled on.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ShowMicrosoftRewards
- GP name: Show Microsoft Rewards experiences
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: ShowMicrosoftRewards
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: ShowMicrosoftRewards
- Example value:

```
<false/>
```

Back to top

ShowOfficeShortcutInFavoritesBar

Show Microsoft Office shortcut in favorites bar (deprecated)

> DEPRECATED: This policy is deprecated. It is currently supported but will become obsolete in a future release.

Supported versions:

- On Windows and macOS since 77 or later

Description

This policy didn't work as expected due to changes in operational requirements. Therefore it's deprecated and should not be used.

Specifies whether to include a shortcut to Office.com in the favorites bar. For users signed into Microsoft Edge the shortcut takes users to their Microsoft Office apps and docs. If you enable or don't configure this policy, users can choose whether to see the shortcut by changing the toggle in the favorites bar context menu. If you disable this policy, the shortcut isn't shown.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ShowOfficeShortcutInFavoritesBar
- GP name: Show Microsoft Office shortcut in favorites bar (deprecated)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ShowOfficeShortcutInFavoritesBar
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: ShowOfficeShortcutInFavoritesBar
- Example value:

```
<false/>
```

Back to top

ShowRecommendationsEnabled

Allow feature recommendations and browser assistance notifications from Microsoft Edge

Supported versions:

- On Windows and macOS since 89 or later

Description

This setting controls the in-browser assistance notifications which are intended to help users get the most out of Microsoft Edge. This is done by recommending features and by helping them use browser features. These notifications take the form of dialog boxes, flyouts, coach marks and banners in the browser. An example of an assistance notification would be when a user has many tabs opened in the browser. In this instance Microsoft Edge may prompt the user to try out the vertical tabs feature which is designed to give better browser tab management.

Disabling this policy will stop this message from appearing again even if the user has too many tabs open. Any features that have been disabled by a management policy are not suggested to users. If you enable or don't configure this setting, users will receive recommendations or notifications from Microsoft Edge. If you disable this setting, users will not receive any recommendations or notifications from Microsoft Edge

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ShowRecommendationsEnabled
- GP name: Allow feature recommendations and browser assistance notifications from Microsoft Edge
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: ShowRecommendationsEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: ShowRecommendationsEnabled
- Example value:

```
<true/>
```

Back to top

SignedHTTPExchangeEnabled

Enable Signed HTTP Exchange (SXG) support

Supported versions:

- On Windows and macOS since 78 or later

Description

Enable support for Signed HTTP Exchange (SXG).

If this policy isn't set or enabled, Microsoft Edge will accept web contents served as Signed HTTP Exchanges.

If this policy is set to disabled, Signed HTTP Exchanges can't be loaded.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SignedHTTPExchangeEnabled
- GP name: Enable Signed HTTP Exchange (SXG) support
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: SignedHTTPExchangeEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: SignedHTTPExchangeEnabled
- Example value:

```
<true/>
```

Back to top

SitePerProcess

Enable site isolation for every site

Supported versions:

- On Windows and macOS since 77 or later

Description

The 'SitePerProcess' policy can be used to prevent users from opting out of the default behavior of isolating all sites. Note that you can also use the IsolateOrigins policy to isolate additional, finer-grained origins.

If you enable this policy, users can't opt out of the default behavior where each site runs in its own process.

If you disable or don't configure this policy, a user can opt out of site isolation. (For example, by using "Disable site isolation" entry in edge://flags.) Disabling the policy or not configuring the policy doesn't turn off Site Isolation.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SitePerProcess
- GP name: Enable site isolation for every site
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: SitePerProcess
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: SitePerProcess
- Example value:

```
<true/>
```

Back to top

SiteSafetyServicesEnabled

Allow users to configure Site safety services

Supported versions:

- On Windows and macOS since 101 or later

Description

This policy disables site safety services from showing top site info in the page info dialog.

If you enable this policy or don't configure it, the top site info will be shown.

If you disable this policy, the top site info will not be shown.

Supported features:

- Can be mandatory: Yes

- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SiteSafetyServicesEnabled
- GP name: Allow users to configure Site safety services
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: SiteSafetyServicesEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: SiteSafetyServicesEnabled
- Example value:

```
<true/>
```

Back to top

SmartActionsBlockList

Block smart actions for a list of services

Supported versions:

- On Windows and macOS since 89 or later

Description

List specific services, such as PDFs, that don't show smart actions. (Smart actions are actions like "define" which are available in full and mini context menus in Microsoft Edge.)

If you enable the policy:

- The smart action in the mini and full context menu will be disabled for all profiles for services that match the given list.
- Users will not see the smart action in the mini and full context menu on text selection for services that match the given list.
- In Microsoft Edge settings, the smart action in the mini and full context menu will be disabled for services that match the given list.

If you disable or don't configure this policy:

- The smart action in the mini and full context menu will be enabled for all profiles.
- Users will see the smart action in the mini and full context menu on text selection.
- In Microsoft Edge settings, the smart action in the mini and full context menu will be enabled.

Policy options mapping:

- smart_actions_pdf (smart_actions_pdf) = Smart actions in PDF

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SmartActionsBlockList
- GP name: Block smart actions for a list of services
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\SmartActionsBlockList
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended\SmartActionsBlockList
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\SmartActionsBlockList\1 = "smart_actions_pdf"
```

Mac information and settings

- Preference Key Name: SmartActionsBlockList
- Example value:

```
<array>
  <string>smart_actions_pdf</string>
</array>
```

Back to top

SpeechRecognitionEnabled

Configure Speech Recognition

Supported versions:

- On Windows and macOS since 87 or later

Description

Set whether websites can use the W3C Web Speech API to recognize speech from the user. The Microsoft Edge implementation of the Web Speech API uses Azure Cognitive Services, so voice data will leave the machine.

If you enable or don't configure this policy, web-based applications that use the Web Speech API can use Speech Recognition.

If you disable this policy, Speech Recognition is not available through the Web Speech API.

Read more about this feature here: SpeechRecognition API: https://go.microsoft.com/fwlink/?linkid=2143388 Cognitive Services: https://go.microsoft.com/fwlink/?linkid=2143680

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SpeechRecognitionEnabled
- GP name: Configure Speech Recognition
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: SpeechRecognitionEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: SpeechRecognitionEnabled
- Example value:

```
<true/>
```

Back to top

SpellcheckEnabled

Enable spellcheck

Supported versions:

- On Windows and macOS since 77 or later

Description

If you enable or don't configure this policy, the user can use spellcheck.

If you disable this policy, the user can't use spellcheck and the SpellcheckLanguage and SpellcheckLanguageBlocklist policies are also disabled.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SpellcheckEnabled
- GP name: Enable spellcheck
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: SpellcheckEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: SpellcheckEnabled
- Example value:

```
<false/>
```

Back to top

SpellcheckLanguage

Enable specific spellcheck languages

Supported versions:

- On Windows since 77 or later

Description

Enables different languages for spellcheck. Any language that you specify that isn't recognized is ignored.

If you enable this policy, spellcheck is enabled for the languages specified, as well as any languages the user has enabled.

If you don't configure or disable this policy, there's no change to the user's spellcheck preferences.

If the SpellcheckEnabled policy is disabled, this policy will have no effect.

If a language is included in both the 'SpellcheckLanguage' and the SpellcheckLanguageBlocklist policy, the spellcheck language is enabled.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SpellcheckLanguage
- GP name: Enable specific spellcheck languages

- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\SpellcheckLanguage
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\SpellcheckLanguage\1 = "fr"
SOFTWARE\Policies\Microsoft\Edge\SpellcheckLanguage\2 = "es"
```

Back to top

SpellcheckLanguageBlocklist

Force disable spellcheck languages

Supported versions:

- On Windows since 78 or later

Description

Force-disables spellcheck languages. Unrecognized languages in that list will be ignored.

If you enable this policy, spellcheck will be disabled for the languages specified. The user can still enable or disable spellcheck for languages not in the list.

If you do not set this policy, or disable it, there will be no change to the user's spellcheck preferences.

If the SpellcheckEnabled policy is set to disabled, this policy will have no effect.

If a language is included in both the SpellcheckLanguage and the 'SpellcheckLanguageBlocklist' policy, the spellcheck language is enabled.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SpellcheckLanguageBlocklist
- GP name: Force disable spellcheck languages
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\SpellcheckLanguageBlocklist
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\SpellcheckLanguageBlocklist\1 = "fr"
SOFTWARE\Policies\Microsoft\Edge\SpellcheckLanguageBlocklist\2 = "es"
```

Back to top

StricterMixedContentTreatmentEnabled

Enable stricter treatment for mixed content (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 84.

Supported versions:

- On Windows and macOS since 81, until 84

Description

This policy doesn't work because it was only intended to be a short-term mechanism to give enterprises more time to update their web content if it was found to be incompatible with stricter mixed content treatment.

This policy controls the treatment for mixed content (HTTP content in HTTPS sites) in the browser.

If you set this policy to true or not set, audio and video mixed content will be automatically upgraded to HTTPS (that is, the URL will be rewritten as HTTPS, without a fallback if the resource isn't available over HTTPS) and a 'Not Secure' warning will be shown in the URL bar for image mixed content.

If you set the policy to false, auto upgrades will be disabled for audio and video, and no warning will be shown for images.

This policy does not affect other types of mixed content other than audio, video, and images.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: StricterMixedContentTreatmentEnabled
- GP name: Enable stricter treatment for mixed content (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: StricterMixedContentTreatmentEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: StricterMixedContentTreatmentEnabled
- Example value:

```
<true/>
```

Back to top

SuppressUnsupportedOSWarning

Suppress the unsupported OS warning

Supported versions:

- On Windows and macOS since 77 or later

Description

Suppresses the warning that appears when Microsoft Edge is running on a computer or operating system that is no longer supported.

If this policy is false or unset, the warnings will appear on such unsupported computers or operating systems.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SuppressUnsupportedOSWarning
- GP name: Suppress the unsupported OS warning
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: SuppressUnsupportedOSWarning
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: SuppressUnsupportedOSWarning
- Example value:

```
<true/>
```

Back to top

SyncDisabled

Disable synchronization of data using Microsoft sync services

Supported versions:

- On Windows and macOS since 77 or later

Description

Disables data synchronization in Microsoft Edge. This policy also prevents the sync consent prompt from appearing.

This policy disables cloud synchronization only and has no impact on the RoamingProfileSupportEnabled policy.

If you don't set this policy or apply it as recommended, users will be able to turn sync on or off. If you apply this policy as mandatory, users will not be able to turn sync on.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SyncDisabled
- GP name: Disable synchronization of data using Microsoft sync services
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: SyncDisabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: SyncDisabled
- Example value:

```
<true/>
```

Back to top

SyncTypesListDisabled

Configure the list of types that are excluded from synchronization

Supported versions:

- On Windows and macOS since 83 or later

Description

If you enable this policy all the specified data types will be excluded from synchronization. This policy can be used to limit the type of data uploaded to the Microsoft Edge synchronization service.

You can provide one of the following data types for this policy: "favorites", "settings", "passwords", "addressesAndMore", "extensions", "history", "openTabs", and "collections". The "apps" data type will be

supported starting in Microsoft Edge version 100. Note that these data type names are case sensitive.

Users will not be able to override the disabled data types.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: SyncTypesListDisabled
- GP name: Configure the list of types that are excluded from synchronization
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\SyncTypesListDisabled
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\SyncTypesListDisabled\1 = "favorites"
```

Mac information and settings

- Preference Key Name: SyncTypesListDisabled
- Example value:

```
<array>
  <string>favorites</string>
</array>
```

Back to top

TLS13HardeningForLocalAnchorsEnabled

Enable a TLS 1.3 security feature for local trust anchors (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 85.

Supported versions:

- On Windows and macOS since 81, until 85

Description

This policy doesn't work because it was only intended to be a short-term mechanism to give enterprises more time to upgrade affected proxies.

This policy controls a security feature in TLS 1.3 that protects connections against downgrade attacks. It is backwards-compatible and will not affect connections to compliant TLS 1.2 servers or proxies. However, older versions of some TLS-intercepting proxies have an implementation flaw which causes them to be incompatible.

If you enable this policy or don't set it, Microsoft Edge will enable these security protections for all connections.

If you disable this policy, Microsoft Edge will disable these security protections for connections authenticated with locally-installed CA certificates. These protections are always enabled for connections authenticated with publicly-trusted CA certificates.

This policy can be used to test for any affected proxies and upgrade them. Affected proxies are expected to fail connections with an error code of ERR_TLS13_DOWNGRADE_DETECTED.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: TLS13HardeningForLocalAnchorsEnabled
- GP name: Enable a TLS 1.3 security feature for local trust anchors (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: TLS13HardeningForLocalAnchorsEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: TLS13HardeningForLocalAnchorsEnabled
- Example value:

```
<true/>
```

Back to top

TLSCipherSuiteDenyList

Specify the TLS cipher suites to disable

Supported versions:

- On Windows and macOS since 85 or later

Description

Configure the list of cipher suites that are disabled for TLS connections.

If you configure this policy, the list of configured cipher suites will not be used when establishing TLS connections.

If you don't configure this policy, the browser will choose which TLS cipher suites to use.

Cipher suite values to be disabled are specified as 16-bit hexadecimal values. The values are assigned by the

Internet Assigned Numbers Authority (IANA) registry.

The TLS 1.3 cipher suite TLS_AES_128_GCM_SHA256 (0x1301) is required for TLS 1.3 and can't be disabled by this policy.

This policy does not affect QUIC-based connections. QUIC can be turned off via the QuicAllowed policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: TLSCipherSuiteDenyList
- GP name: Specify the TLS cipher suites to disable
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\TLSCipherSuiteDenyList
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\TLSCipherSuiteDenyList\1 = "0x1303"
SOFTWARE\Policies\Microsoft\Edge\TLSCipherSuiteDenyList\2 = "0xcca8"
SOFTWARE\Policies\Microsoft\Edge\TLSCipherSuiteDenyList\3 = "0xcca9"
```

Mac information and settings

- Preference Key Name: TLSCipherSuiteDenyList
- Example value:

```
<array>
  <string>0x1303</string>
  <string>0xcca8</string>
  <string>0xcca9</string>
</array>
```

Back to top

TabFreezingEnabled

Allow freezing of background tabs (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 86.

Supported versions:

- On Windows and macOS since 79, until 86

Description

This policy doesn't work, use SleepingTabsEnabled instead.

Controls whether Microsoft Edge can freeze tabs that are in the background for at least 5 minutes.

Tab freezing reduces CPU, battery, and memory usage. Microsoft Edge uses heuristics to avoid freezing tabs that do useful work in the background, such as display notifications, play sound, and stream video.

If you enable or don't configure this policy, tabs that have been in the background for at least 5 minutes might be frozen.

If you disable this policy, no tabs will be frozen.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: TabFreezingEnabled
- GP name: Allow freezing of background tabs (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: TabFreezingEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: TabFreezingEnabled
- Example value:

```
<false/>
```

Back to top

TargetBlankImpliesNoOpener

Do not set window.opener for links targeting _blank (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 102.

Supported versions:

- On Windows and macOS since 88, until 102

Description

If you enable this policy or leave it unset, the window.opener property is set to null unless the anchor specifies

rel="opener".

If you disable this policy, popups that target _blank are permitted to access (via JavaScript) the page that requested to open the popup.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: TargetBlankImpliesNoOpener
- GP name: Do not set window.opener for links targeting _blank (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: TargetBlankImpliesNoOpener
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: TargetBlankImpliesNoOpener
- Example value:

```
<false/>
```

Back to top

TaskManagerEndProcessEnabled

Enable ending processes in the Browser task manager

Supported versions:

- On Windows and macOS since 77 or later

Description

If you enable or don't configure this policy, users can end processes in the Browser task manager. If you disable it, users can't end processes, and the End process button is disabled in the Browser task manager.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: TaskManagerEndProcessEnabled
- GP name: Enable ending processes in the Browser task manager
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: TaskManagerEndProcessEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: TaskManagerEndProcessEnabled
- Example value:

```
<true/>
```

Back to top

TextPredictionEnabled

Text prediction enabled by default

Supported versions:

- On Windows and macOS since 104 or later

Description

The Microsoft Turing service uses natural language processing to generate predictions for long-form editable text fields on web pages.

If you enable or don't configure this policy, text predictions will be provided for eligible text fields.

If you disable this policy, text predictions will not be provided in eligible text fields. Sites may still provide their own text predictions.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: TextPredictionEnabled
- GP name: Text prediction enabled by default
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: TextPredictionEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: TextPredictionEnabled
- Example value:

```
<false/>
```

Back to top

TotalMemoryLimitMb

Set limit on megabytes of memory a single Microsoft Edge instance can use

Supported versions:

- On Windows and macOS since 80 or later

Description

Configures the amount of memory that a single Microsoft Edge instance can use before tabs start getting discarded to save memory. The memory used by the tab will be freed and the tab will have to be reloaded when switched to.

If you enable this policy, the browser will start to discard tabs to save memory once the limitation is exceeded. However, there is no guarantee that the browser is always running under the limit. Any value under 1024 will be rounded up to 1024.

If you don't set this policy, the browser will only attempt to save memory when it has detected that the amount of physical memory on its machine is low.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: TotalMemoryLimitMb
- GP name: Set limit on megabytes of memory a single Microsoft Edge instance can use
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: TotalMemoryLimitMb

- Value Type: REG_DWORD

Example value:

```
0x00000800
```

Mac information and settings

- Preference Key Name: TotalMemoryLimitMb
- Example value:

```
<integer>2048</integer>
```

Back to top

TrackingPrevention

Block tracking of users' web-browsing activity

Supported versions:

- On Windows and macOS since 78 or later

Description

Lets you decide whether to block websites from tracking users' web-browsing activity.

If you disable this policy or don't configure it, users can set their own level of tracking prevention.

Policy options mapping:

- TrackingPreventionOff (0) = Off (no tracking prevention)
- TrackingPreventionBasic (1) = Basic (blocks harmful trackers, content and ads will be personalized)
- TrackingPreventionBalanced (2) = Balanced (blocks harmful trackers and trackers from sites user has not visited; content and ads will be less personalized)
- TrackingPreventionStrict (3) = Strict (blocks harmful trackers and majority of trackers from all sites; content and ads will have minimal personalization. Some parts of sites might not work)

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: TrackingPrevention
- GP name: Block tracking of users' web-browsing activity
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: TrackingPrevention

- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Mac information and settings

- Preference Key Name: TrackingPrevention
- Example value:

```
<integer>2</integer>
```

Back to top

TranslateEnabled

Enable Translate

Supported versions:

- On Windows and macOS since 77 or later

Description

Enables the integrated Microsoft translation service on Microsoft Edge.

If you enable this policy, Microsoft Edge offers translation functionality to the user by showing an integrated translate flyout when appropriate, and a translate option on the right-click context menu.

Disable this policy to disable all built-in translate features.

If you don't configure the policy, users can choose whether to use the translation functionality or not.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: TranslateEnabled
- GP name: Enable Translate
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: TranslateEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: TranslateEnabled
- Example value:

```
<true/>
```

Back to top

TravelAssistanceEnabled

Enable travel assistance (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 105.

Supported versions:

- On Windows and macOS since 93, until 105

Description

This policy is obsolete as the feature is now contained within the Edge Sidebar and can be managed using the HubsSidebarEnabled policy. It doesn't work in Microsoft Edge after version 105. Configure this policy to allow/disallow travel assistance.

The travel assistance feature gives helpful and relevant information to a user who performs Travel related task within the browser. This feature provides trusted and validated suggestions / information to the users from across sources gathered by Microsoft.

If you enable or don't configure this setting, travel assistance will be enabled for the users when they are performing travel related tasks.

If you disable this setting, travel assistance will be disabled and users will not be able to see any travel related recommendations.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: TravelAssistanceEnabled
- GP name: Enable travel assistance (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: TravelAssistanceEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: TravelAssistanceEnabled
- Example value:

```
<true/>
```

Back to top

TripleDESEnabled

Enable 3DES cipher suites in TLS

Supported versions:

- On Windows and macOS since 93 or later

Description

'Warning: 3DES will be completely removed from Microsoft Edge in version 95 (around October 2021) and this policy will stop working then.

If the policy is set to true, then 3DES cipher suites in TLS will be enabled. If it is set to false, they will be disabled. If the policy is unset, 3DES cipher suites are disabled by default. This policy may be used to temporarily retain compatibility with an outdated server. This is a stopgap measure and the server should be reconfigured.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: TripleDESEnabled
- GP name: Enable 3DES cipher suites in TLS
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: TripleDESEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: TripleDESEnabled
- Example value:

```
<false/>
```

Back to top

U2fSecurityKeyApiEnabled

Allow using the deprecated U2F Security Key API (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 103.

Supported versions:

- On Windows and macOS since 98, until 103

Description

This policy is obsolete because it was intended to be a short-term mechanism to give enterprises more time to update their web content when it's found to be incompatible with the change to remove the U2F Security Key API. It doesn't work in Microsoft Edge after version 103.

If you enable this policy, the deprecated U2F Security Key API can be used and the deprecation reminder prompt shown for U2F API requests is suppressed.

If you disable this policy or don't configure it, the U2F Security Key API is disabled by default and can only be used by sites that register for and use the U2FSecurityKeyAPI origin trial which ended after Microsoft Edge version 103.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: U2fSecurityKeyApiEnabled
- GP name: Allow using the deprecated U2F Security Key API (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: U2fSecurityKeyApiEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: U2fSecurityKeyApiEnabled
- Example value:

```
<true/>
```

Back to top

URLAllowlist

Define a list of allowed URLs

Supported versions:

- On Windows and macOS since 77 or later

Description

Setting the policy provides access to the listed URLs, as exceptions to URLBlocklist.

Format the URL pattern according to https://go.microsoft.com/fwlink/?linkid=2095322.

You can use this policy to open exceptions to restrictive block lists. For example, you can include '*' in the block list to block all requests, and then use this policy to allow access to a limited list of URLs. You can use this policy to open exceptions to certain schemes, subdomains of other domains, ports, or specific paths.

The most specific filter determines if a URL is blocked or allowed. The allowed list takes precedence over the block list.

This policy is limited to 1000 entries; subsequent entries are ignored.

This policy also allows the browser to automatically invoke external applications registered as protocol handlers for protocols like "tel:" or "ssh:".

If you don't configure this policy, there are no exceptions to the block list in the URLBlocklist policy.

This policy does not work as expected with file://* wildcards.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: URLAllowlist
- GP name: Define a list of allowed URLs
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\URLAllowlist
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\URLAllowlist\1 = "contoso.com"
SOFTWARE\Policies\Microsoft\Edge\URLAllowlist\2 = "https://ssl.server.com"
SOFTWARE\Policies\Microsoft\Edge\URLAllowlist\3 = "hosting.com/good_path"
SOFTWARE\Policies\Microsoft\Edge\URLAllowlist\4 = "https://server:8080/path"
SOFTWARE\Policies\Microsoft\Edge\URLAllowlist\5 = ".exact.hostname.com"
```

Mac information and settings

- Preference Key Name: URLAllowlist
- Example value:

```
<array>
  <string>contoso.com</string>
  <string>https://ssl.server.com</string>
  <string>hosting.com/good_path</string>
  <string>https://server:8080/path</string>
  <string>.exact.hostname.com</string>
</array>
```

Back to top

URLBlocklist

Block access to a list of URLs

Supported versions:

- On Windows and macOS since 77 or later

Description

Define a list of sites, based on URL patterns, that are blocked (your users can't load them).

Format the URL pattern according to https://go.microsoft.com/fwlink/?linkid=2095322.

You can define exceptions in the URLAllowlist policy. These policies are limited to 1000 entries; subsequent entries are ignored.

Note that blocking internal 'edge://*' URLs isn't recommended - this may lead to unexpected errors.

This policy doesn't prevent the page from updating dynamically through JavaScript. For example, if you block 'contoso.com/abc', users might still be able to visit 'contoso.com' and click on a link to visit 'contoso.com/abc', as long as the page doesn't refresh.

If you don't configure this policy, no URLs are blocked.

This policy does not work as expected with file://* wildcards.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: URLBlocklist
- GP name: Block access to a list of URLs
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\URLBlocklist
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\URLBlocklist\1 = "contoso.com"
SOFTWARE\Policies\Microsoft\Edge\URLBlocklist\2 = "https://ssl.server.com"
SOFTWARE\Policies\Microsoft\Edge\URLBlocklist\3 = "hosting.com/bad_path"
SOFTWARE\Policies\Microsoft\Edge\URLBlocklist\4 = "https://server:8080/path"
SOFTWARE\Policies\Microsoft\Edge\URLBlocklist\5 = ".exact.hostname.com"
SOFTWARE\Policies\Microsoft\Edge\URLBlocklist\6 = "custom_scheme:*"
SOFTWARE\Policies\Microsoft\Edge\URLBlocklist\7 = "*"
```

Mac information and settings

- Preference Key Name: URLBlocklist
- Example value:

```
<array>
  <string>contoso.com</string>
  <string>https://ssl.server.com</string>
  <string>hosting.com/bad_path</string>
  <string>https://server:8080/path</string>
  <string>.exact.hostname.com</string>
  <string>custom_scheme:*</string>
  <string>*</string>
</array>
```

Back to top

UnthrottledNestedTimeoutEnabled

JavaScript setTimeout will not be clamped until a higher nesting threshold is set (deprecated)

> DEPRECATED: This policy is deprecated. It is currently supported but will become obsolete in a future release.

Supported versions:

- On Windows and macOS since 105 or later

Description

This policy is deprecated because it is a temporary policy for web standards compliance. It won't work in Microsoft Edge as soon as version 107. If you enable this policy, the JavaScript setTimeout and setInterval, with an interval smaller than 4ms, will not be clamped. This improves short horizon performance, but websites abusing the API will still eventually have their setTimeout usages clamped. If you disable or don't configure policy, the JavaScript setTimeout and setInterval, with an interval smaller than 4ms, will be clamped.

This is a web standards compliancy feature that may change task ordering on a web page, leading to unexpected behavior on sites that are dependent on a certain ordering. It also may affect sites with a lot of usage of a timeout of 0ms for setTimeout. For example, increasing CPU load.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: UnthrottledNestedTimeoutEnabled
- GP name: JavaScript setTimeout will not be clamped until a higher nesting threshold is set (deprecated)

- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: UnthrottledNestedTimeoutEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: UnthrottledNestedTimeoutEnabled
- Example value:

```
<true/>
```

Back to top

UpdatePolicyOverride

Specifies how Microsoft Edge Update handles available updates from Microsoft Edge

Supported versions:

- On macOS since 89 or later

Description

If you enable this policy, Microsoft Edge Update handles Microsoft Edge updates according to how you configure the following options:

- Automatic silent updates only: Updates are applied only when they're found by the periodic update check.
- Manual updates only: Updates are applied only when the user runs a manual update check. (Not all apps provide an interface for this option.)

If you select manual updates, make sure you periodically check for updates by using Microsoft Autoupdate.

If you don't enable and configure this policy, Microsoft Edge Update automatically checks for updates.

Policy options mapping:

- automatic-silent-only (automatic-silent-only) = Updates are applied only when they're found by the periodic update check.
- manual-only (manual-only) = Updates are applied only when the user runs a manual update check. (Not all apps provide an interface for this option.)

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- String

Mac information and settings

- Preference Key Name: UpdatePolicyOverride
- Example value:

```
<string>automatic-silent-only</string>
```

Back to top

UserAgentClientHintsEnabled

Enable the User-Agent Client Hints feature (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 93.

Supported versions:

- On Windows and macOS since 86, until 93

Description

This policy is obsolete because it was intended for short-term adaptation purposes only. It doesn't work in Microsoft Edge after version 93.

When enabled the User-Agent Client Hints feature sends granular request headers that provide information about the user browser (for example, the browser version) and environment (for example, the system architecture).

This is an additive feature, but the new headers may break some websites that restrict the characters that requests may contain.

If you enable or don't configure this policy, the User-Agent Client Hints feature is enabled. If you disable this policy, this feature is unavailable.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: UserAgentClientHintsEnabled
- GP name: Enable the User-Agent Client Hints feature (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: UserAgentClientHintsEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: UserAgentClientHintsEnabled
- Example value:

```
<true/>
```

Back to top

UserAgentClientHintsGREASEUpdateEnabled

Control the User-Agent Client Hints GREASE Update feature

Supported versions:

- On Windows and macOS since 102 or later

Description

The User-Agent GREASE specification recommends the inclusion of additional GREASE characters beyond the current semicolon and space, and recommends that the arbitrary version number be varied over time.

When enabled, the User-Agent Client Hints GREASE Update feature aligns the User-Agent GREASE algorithm with the latest version from the specification. The updated specification may break some websites that restrict the characters that requests may contain. For more information, see the following specification: https://wicg.github.io/ua-client-hints/#grease

If this policy is enabled or not configured, the User-Agent GREASE algorithm from the specification will be used. If the policy is disabled, the prior User-Agent GREASE algorithm will be used.

This policy is a temporary measure and will be removed in a future release.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: UserAgentClientHintsGREASEUpdateEnabled
- GP name: Control the User-Agent Client Hints GREASE Update feature
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: UserAgentClientHintsGREASEUpdateEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: UserAgentClientHintsGREASEUpdateEnabled
- Example value:

```
<true/>
```

Back to top

UserAgentReduction

Enable or disable the User-Agent Reduction

Supported versions:

- On Windows and macOS since 99 or later

Description

The User-Agent HTTP request header is scheduled to be reduced. To facilitate testing and compatibility, this policy can enable the reduction feature for all websites, or disable the ability for origin trials, or field trials to enable the feature.

If you don't configure this policy or set it to Default, User-Agent will be controlled by experimentation.

Set this policy to 'ForceEnabled' to force the reduced version of the User-Agent request header.

Set this policy to 'ForceDisabled' to force the full version of the User-Agent request header.

To learn more about the User-Agent string, read here:

https://go.microsoft.com/fwlink/?linkid=2186267

Policy options mapping:

- Default (0) = User-Agent reduction will be controllable via Experimentation
- ForceDisabled (1) = User-Agent reduction diabled, and not enabled by Experimentation
- ForceEnabled (2) = User-Agent reduction will be enabled for all origins

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: UserAgentReduction
- GP name: Enable or disable the User-Agent Reduction
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: UserAgentReduction
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: UserAgentReduction
- Example value:

```
<integer>0</integer>
```

Back to top

UserDataDir

Set the user data directory

Supported versions:

- On Windows and macOS since 77 or later

Description

Set the directory to use for storing user data.

If you enable this policy, Microsoft Edge uses the specified directory regardless of whether the user has set the '--user-data-dir' command-line flag.

If you don't enable this policy, the default profile path is used, but the user can override it by using the '--user-data-dir' flag. Users can find the directory for the profile at edge://version/ under profile path.

To avoid data loss or other errors, don't configure this policy to a volume's root directory or to a directory that's used for other purposes, because Microsoft Edge manages its contents.

See https://go.microsoft.com/fwlink/?linkid=2095041 for a list of variables that can be used.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: UserDataDir
- GP name: Set the user data directory
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: UserDataDir
- Value Type: REG_SZ

Example value:

```
"${users}/${user_name}/Edge"
```

Mac information and settings

- Preference Key Name: UserDataDir
- Example value:

```
<string>${users}/${user_name}/Edge</string>
```

Back to top

UserDataSnapshotRetentionLimit

Limits the number of user data snapshots retained for use in case of emergency rollback

Supported versions:

- On Windows since 86 or later

Description

Following each major version update, Microsoft Edge will create a snapshot of parts of the user's browsing data to use in case of a later emergency that requires a temporary version rollback. If a temporary rollback is performed to a version for which a user has a corresponding snapshot, the data in the snapshot is restored. This lets users keep settings such as bookmarks and autofill data.

If you don't set this policy, the default value of 3 snapshots is used.

If you set this policy, old snapshots are deleted as needed to respect the limit you set. If you set this policy to 0, no snapshots are taken.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: UserDataSnapshotRetentionLimit
- GP name: Limits the number of user data snapshots retained for use in case of emergency rollback
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: UserDataSnapshotRetentionLimit
- Value Type: REG_DWORD

Example value:

```
0x00000003
```

Back to top

UserFeedbackAllowed

Allow user feedback

Supported versions:

- On Windows and macOS since 77 or later

Description

Microsoft Edge uses the Edge Feedback feature (enabled by default) to allow users to send feedback, suggestions or customer surveys and to report any issues with the browser. Also, by default, users can't disable (turn off) the Edge Feedback feature.

Starting in Microsoft Edge 105, if the user is signed into Microsoft Edge with their work or school account, their feedback is associated with their account and organization.

If you enable this policy or don't configure it, users can invoke Edge Feedback.

If you disable this policy, users can't invoke Edge Feedback.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: UserFeedbackAllowed
- GP name: Allow user feedback
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: UserFeedbackAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: UserFeedbackAllowed
- Example value:

```
<true/>
```

Back to top

VerticalTabsAllowed

Configures availability of a vertical layout for tabs on the side of the browser

Supported versions:

- On Windows and macOS since 88 or later

Description

Configures whether a user can access an alternative layout where tabs are vertically aligned on the side of the browser instead of at the top. When there are several tabs open, this layout provides better tab viewing and management. There's better visibility of the site titles, it's easier to scan aligned icons, and there's more space to manage and close tabs.

If you disable this policy, then the vertical tab layout will not be available as an option for users.

If you enable or don't configure this policy, the tab layout will still be at the top, but a user has the option to turn on vertical tabs on the side.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: VerticalTabsAllowed
- GP name: Configures availability of a vertical layout for tabs on the side of the browser
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: VerticalTabsAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: VerticalTabsAllowed
- Example value:

```
<true/>
```

Back to top

VideoCaptureAllowed

Allow or block video capture

Supported versions:

- On Windows and macOS since 77 or later

Description

Control whether sites can capture video.

If enabled or not configured (default), the user will be asked about video capture access for all sites except those with URLs configured in the VideoCaptureAllowedUrls policy list, which will be granted access without prompting.

If you disable this policy, the user isn't prompted, and video capture is only available to URLs configured in VideoCaptureAllowedUrls policy.

This policy affects all types of video inputs, not only the built-in camera.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: VideoCaptureAllowed
- GP name: Allow or block video capture
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: VideoCaptureAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: VideoCaptureAllowed
- Example value:

```
<false/>
```

Back to top

VideoCaptureAllowedUrls

Sites that can access video capture devices without requesting permission

Supported versions:

- On Windows and macOS since 77 or later

Description

Specify websites, based on URL patterns, that can use video capture devices without asking the user for permission. Patterns in this list are matched against the security origin of the requesting URL. If they match, the site is automatically granted access to video capture devices.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: VideoCaptureAllowedUrls
- GP name: Sites that can access video capture devices without requesting permission

- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\VideoCaptureAllowedUrls
- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\VideoCaptureAllowedUrls\1 = "https://www.contoso.com/"
SOFTWARE\Policies\Microsoft\Edge\VideoCaptureAllowedUrls\2 = "https://[*.]contoso.edu/"
```

Mac information and settings

- Preference Key Name: VideoCaptureAllowedUrls
- Example value:

```
<array>
  <string>https://www.contoso.com/</string>
  <string>https://[*.]contoso.edu/</string>
</array>
```

Back to top

VisualSearchEnabled

Visual search enabled

Supported versions:

- On Windows since 95 or later

Description

Visual search lets you quickly explore more related content about entities in an image.

If you enable or don't configure this policy, visual search will be enabled via image hover, context menu, and search in sidebar.

If you disable this policy, visual search will be disabled and you won't be able to get more info about images via hover, context menu, and search in sidebar.

Note: Visual Search in Web Capture is still managed by WebCaptureEnabled policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: Yes
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: VisualSearchEnabled
- GP name: Visual search enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): Administrative Templates/Microsoft Edge - Default Settings (users can override)/

- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): SOFTWARE\Policies\Microsoft\Edge\Recommended
- Value Name: VisualSearchEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Back to top

WPADQuickCheckEnabled

Set WPAD optimization

Supported versions:

- On Windows and macOS since 77 or later

Description

Allows you to turn off WPAD (Web Proxy Auto-Discovery) optimization in Microsoft Edge.

If you disable this policy, WPAD optimization is disabled, which makes the browser wait longer for DNS-based WPAD servers.

If you enable or don't configure the policy, WPAD optimization is enabled.

Independent of whether or how this policy is enabled, the WPAD optimization setting cannot be changed by users.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WPADQuickCheckEnabled
- GP name: Set WPAD optimization
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: WPADQuickCheckEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: WPADQuickCheckEnabled
- Example value:

```
<true/>
```

Back to top

WebAppInstallForceList

Configure list of force-installed Web Apps

Supported versions:

- On Windows and macOS since 80 or later

Description

Configure this policy to specify a list of web apps that install silently, without user interaction, and which users can't uninstall or turn off.

Each list item of the policy is an object with a mandatory member: url (the URL of the web app to install)

and 5 optional members:

- default_launch_container (specifies the window mode that the web app opens with-a new tab is the default.)
- create_desktop_shortcut (True if you want to create Linux and Microsoft Windows desktop shortcuts).
- fallback_app_name (Starting with Microsoft Edge version 90, allows you to override the app name if it is not a Progressive Web App (PWA), or the app name that is temporarily installed if it is a PWA but authentication is required before the installation can be completed. If both custom_name and fallback_app_name are provided, the latter will be ignored.)
- custom_name (Allows you to permanently override the app name for all web apps and PWAs. Not currently supported in Microsoft Edge.)
- custom_icon (Allows you to override the app icon of installed apps. The icons have to be square, maximal 1 MB in size, and in one of the following formats: jpeg, png, gif, webp, ico. The hash value has to be the SHA256 hash of the icon file. Not currently supported in Microsoft Edge.)
- install_as_shortcut (Starting with Microsoft Edge version 107). If enabled the given url will be installed as a shortcut, as if done via the "Create Shortcut..." option in the desktop browser GUI. Note that when installed as a shortcut it won't be updated if the manifest in url changes. If disabled or unset, the web app at the given url will be installed normally. Not currently supported in Microsoft Edge.)

  Supported features:

  - Can be mandatory: Yes
  - Can be recommended: No
  - Dynamic Policy Refresh: Yes

  Data Type:

  - Dictionary

  Windows information and settings

  Group Policy (ADMX) info

  - GP unique name: WebAppInstallForceList
  - GP name: Configure list of force-installed Web Apps
  - GP path (Mandatory): Administrative Templates/Microsoft Edge/
  - GP path (Recommended): N/A
  - GP ADMX file name: MSEdge.admx

  Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: WebAppInstallForceList
- Value Type: REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\WebAppInstallForceList = [
  {
    "create_desktop_shortcut": true,
    "default_launch_container": "window",
    "url": "https://www.contoso.com/maps"
  },
  {
    "default_launch_container": "tab",
    "url": "https://app.contoso.edu"
  },
  {
    "default_launch_container": "window",
    "fallback_app_name": "Editor",
    "url": "https://app.contoso.edu/editor"
  },
  {
    "custom_name": "Spreadsheets",
    "default_launch_container": "window",
    "install_as_shortcut": true,
    "url": "https://app.contoso.edu/sheets"
  },
  {
    "custom_icon": {
      "hash": "c28f469c450e9ab2b86ea47038d2b324c6ad3b1e9a4bd8960da13214afd0ca38",
      "url": "https://mydomain.example.com/sunny_icon.png"
    },
    "url": "https://weather.example.com"
  }
]
```

Compact example value:

```
SOFTWARE\Policies\Microsoft\Edge\WebAppInstallForceList = [{"create_desktop_shortcut": true,
"default_launch_container": "window", "url": "https://www.contoso.com/maps"}, {"default_launch_container":
"tab", "url": "https://app.contoso.edu"}, {"default_launch_container": "window", "fallback_app_name":
"Editor", "url": "https://app.contoso.edu/editor"}, {"custom_name": "Spreadsheets",
"default_launch_container": "window", "install_as_shortcut": true, "url": "https://app.contoso.edu/sheets"},
{"custom_icon": {"hash": "c28f469c450e9ab2b86ea47038d2b324c6ad3b1e9a4bd8960da13214afd0ca38", "url":
"https://mydomain.example.com/sunny_icon.png"}, "url": "https://weather.example.com"}]
```

Mac information and settings

- Preference Key Name: WebAppInstallForceList
- Example value:

```
<key>WebAppInstallForceList</key>
<array>
  <dict>
    <key>create_desktop_shortcut</key>
    <true/>
    <key>default_launch_container</key>
    <string>window</string>
    <key>url</key>
    <string>https://www.contoso.com/maps</string>
  </dict>
  <dict>
    <key>default_launch_container</key>
    <string>tab</string>
    <key>url</key>
    <string>https://app.contoso.edu</string>
  </dict>
  <dict>
    <key>default_launch_container</key>
    <string>window</string>
    <key>fallback_app_name</key>
    <string>Editor</string>
    <key>url</key>
    <string>https://app.contoso.edu/editor</string>
  </dict>
  <dict>
    <key>custom_name</key>
    <string>Spreadsheets</string>
    <key>default_launch_container</key>
    <string>window</string>
    <key>install_as_shortcut</key>
    <true/>
    <key>url</key>
    <string>https://app.contoso.edu/sheets</string>
  </dict>
  <dict>
    <key>custom_icon</key>
    <dict>
      <key>hash</key>
      <string>c28f469c450e9ab2b86ea47038d2b324c6ad3b1e9a4bd8960da13214afd0ca38</string>
      <key>url</key>
      <string>https://mydomain.example.com/sunny_icon.png</string>
    </dict>
    <key>url</key>
    <string>https://weather.example.com</string>
  </dict>
</array>
```

Back to top

WebCaptureEnabled

Enable web capture feature in Microsoft Edge

Supported versions:

- On Windows and macOS since 87 or later

Description

Enables the web capture feature in Microsoft Edge that allows users to capture web and PDF content, and annotate the capture using inking tools. Starting with Microsoft Edge version 107, users can also perform visual image search on the captured content.

If you enable this policy or don't configure it, the Web capture option shows up in the context menu, Settings and more menu, and by using the keyboard shortcut, CTRL+SHIFT+S. If you disable this policy, users can't access the web capture feature in Microsoft Edge.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WebCaptureEnabled
- GP name: Enable web capture feature in Microsoft Edge
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: WebCaptureEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: WebCaptureEnabled
- Example value:

```
<true/>
```

Back to top

WebComponentsV0Enabled

Re-enable Web Components v0 API until M84 (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 84.

Supported versions:

- On Windows and macOS since 80, until 84

Description

This policy doesn't work because this policy allowed these features to be selectively re-enabled until Microsoft Edge version 85. The Web Components v0 APIs (Shadow DOM v0, Custom Elements v0, and HTML Imports) were deprecated in 2018, and have been disabled by default starting in Microsoft Edge version 80.

If you set this policy is set to True, the Web Components v0 features will be enabled for all sites.

If you set this policy to False or don't set this policy, the Web Components v0 features will be disabled by default, starting in Microsoft Edge version 80.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WebComponentsV0Enabled
- GP name: Re-enable Web Components v0 API until M84 (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: WebComponentsV0Enabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: WebComponentsV0Enabled
- Example value:

```
<true/>
```

Back to top

WebDriverOverridesIncompatiblePolicies

Allow WebDriver to Override Incompatible Policies (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 84.

Supported versions:

- On Windows and macOS since 77, until 84

Description

This policy doesn't work because WebDriver is now compatible with all existing policies.

This policy allows users of the WebDriver feature to override policies which can interfere with its operation.

Currently this policy disables SitePerProcess and IsolateOrigins policies.

If the policy is enabled, WebDriver will be able to override incomaptible policies. If the policy is disabled or not configured, WebDriver will not be allowed to override incompatible policies.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WebDriverOverridesIncompatiblePolicies
- GP name: Allow WebDriver to Override Incompatible Policies (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: WebDriverOverridesIncompatiblePolicies
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: WebDriverOverridesIncompatiblePolicies
- Example value:

```
<true/>
```

Back to top

WebRtcAllowLegacyTLSProtocols

Allow legacy TLS/DTLS downgrade in WebRTC (deprecated)

> DEPRECATED: This policy is deprecated. It is currently supported but will become obsolete in a future release.

Supported versions:

- On Windows and macOS since 88 or later

Description

If you enable this policy, WebRTC peer connections can downgrade to obsolete versions of the TLS/DTLS (DTLS 1.0, TLS 1.0 and TLS 1.1) protocols. If you disable or don't set this policy, these TLS/DTLS versions are disabled.

This policy is temporary and will be removed in a future version of Microsoft Edge.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WebRtcAllowLegacyTLSProtocols
- GP name: Allow legacy TLS/DTLS downgrade in WebRTC (deprecated)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: WebRtcAllowLegacyTLSProtocols
- Value Type: REG_DWORD

Example value:

```
0x00000000
```

Mac information and settings

- Preference Key Name: WebRtcAllowLegacyTLSProtocols
- Example value:

```
<false/>
```

Back to top

WebRtcLocalIpsAllowedUrls

Manage exposure of local IP addressess by WebRTC

Supported versions:

- On Windows and macOS since 80 or later

Description

Specifies a list of origins (URLs) or hostname patterns (like "*contoso.com*") for which local IP address should be exposed by WebRTC.

If you enable this policy and set a list of origins (URLs) or hostname patterns, when edge://flags/#enable-webrtc-hide-local-ips-with-mdns is Enabled, WebRTC will expose the local IP address for cases that match patterns in the list.

If you disable or don't configure this policy, and edge://flags/#enable-webrtc-hide-local-ips-with-mdns is Enabled, WebRTC will not expose local IP addresses. The local IP address is concealed with an mDNS hostname.

If you enable, disable, or don't configure this policy, and edge://flags/#enable-webrtc-hide-local-ips-with-mdns is Disabled, WebRTC will expose local IP addresses.

Please note that this policy weakens the protection of local IP addresses that might be needed by administrators.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WebRtcLocalIpsAllowedUrls
- GP name: Manage exposure of local IP addressess by WebRTC
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\WebRtcLocalIpsAllowedUrls

- Path (Recommended): N/A
- Value Name: 1, 2, 3, ...
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\WebRtcLocalIpsAllowedUrls\1 = "https://www.contoso.com"
SOFTWARE\Policies\Microsoft\Edge\WebRtcLocalIpsAllowedUrls\2 = "*contoso.com*"
```

Mac information and settings

- Preference Key Name: WebRtcLocalIpsAllowedUrls
- Example value:

```
<array>
  <string>https://www.contoso.com</string>
  <string>*contoso.com*</string>
</array>
```

Back to top

WebRtcLocalhostIpHandling

Restrict exposure of local IP address by WebRTC

Supported versions:

- On Windows and macOS since 77 or later

Description

Allows you to set whether or not WebRTC exposes the user's local IP address.

If you set this policy to "AllowAllInterfaces" or "AllowPublicAndPrivateInterfaces", WebRTC exposes the local IP address.

If you set this policy to "AllowPublicInterfaceOnly" or "DisableNonProxiedUdp", WebRTC doesn't expose the local IP address.

If you don't set this policy, or if you disable it, WebRTC exposes the local IP address.

Note: This policy does not provide an option to exclude specific domains.

Policy options mapping:

- AllowAllInterfaces (default) = Allow all interfaces. This exposes the local IP address
- AllowPublicAndPrivateInterfaces (default_public_and_private_interfaces) = Allow public and private interfaces over http default route. This exposes the local IP address
- AllowPublicInterfaceOnly (default_public_interface_only) = Allow public interface over http default route. This doesn't expose the local IP address
- DisableNonProxiedUdp (disable_non_proxied_udp) = Use TCP unless proxy server supports UDP. This doesn't expose the local IP address

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WebRtcLocalhostIpHandling
- GP name: Restrict exposure of local IP address by WebRTC
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: WebRtcLocalhostIpHandling
- Value Type: REG_SZ

Example value:

```
"default"
```

Mac information and settings

- Preference Key Name: WebRtcLocalhostIpHandling
- Example value:

```
<string>default</string>
```

Back to top

WebRtcRespectOsRoutingTableEnabled

Enable support for Windows OS routing table rules when making peer to peer connections via WebRTC

Supported versions:

- On Windows since 94 or later

Description

Controls whether WebRTC will respect the Windows OS routing table rules when making peer to peer connections, thus enabling split tunnel VPNs.

If you disable this policy or don't configure it, WebRTC will not consider the routing table and may make peer to peer connections over any available network.

If you enable this policy, WebRTC will prefer to make peer to peer connections using the indicated network interface for the remote address as indicated in the routing table.

This policy is only available on Windows.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WebRtcRespectOsRoutingTableEnabled

- GP name: Enable support for Windows OS routing table rules when making peer to peer connections via WebRTC
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: WebRtcRespectOsRoutingTableEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

WebRtcUdpPortRange

Restrict the range of local UDP ports used by WebRTC

Supported versions:

- On Windows and macOS since 77 or later

Description

Restricts the UDP port range used by WebRTC to a specified port interval (endpoints included).

By configuring this policy, you specify the range of local UDP ports that WebRTC can use.

If you don't configure this policy, or if you set it to an empty string or invalid port range, WebRTC can use any available local UDP port.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- String

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WebRtcUdpPortRange
- GP name: Restrict the range of local UDP ports used by WebRTC
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: WebRtcUdpPortRange
- Value Type: REG_SZ

Example value:

```
"10000-11999"
```

Mac information and settings

- Preference Key Name: WebRtcUdpPortRange
- Example value:

```
<string>10000-11999</string>
```

Back to top

WebSQLAccess

Force WebSQL to be enabled

Supported versions:

- On Windows and macOS since 107 or later

Description

WebSQL is on by default as of Microsoft Edge version 101, but can be disabled via a Microsoft Edge flag. If you enable this policy, WebSQL cannot be disabled. If you disable or don't configure this policy, WebSQL can be disabled.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WebSQLAccess
- GP name: Force WebSQL to be enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: WebSQLAccess
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: WebSQLAccess
- Example value:

```
<true/>
```

Back to top

WebSQLInThirdPartyContextEnabled

Force WebSQL in third-party contexts to be re-enabled (obsolete)

> OBSOLETE: This policy is obsolete and doesn't work after Microsoft Edge 100.

Supported versions:

- On Windows and macOS since 97, until 100

Description

This policy is obsolete because it was intended to be a short-term mechanism to give enterprises more time to update their web content when it's found to be incompatible with the change to disable WebSQL in third-party contexts. It doesn't work in Microsoft Edge after version 100.

WebSQL in third-party contexts (for example, cross-site iframes) is off by default as of Microsoft Edge version 97 and was fully removed in version 101.

If you enable this policy, WebSQL in third-party contexts will be re-enabled.

If you disable this policy or don't configure it, WebSQL in third-party contexts will stay off.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WebSQLInThirdPartyContextEnabled
- GP name: Force WebSQL in third-party contexts to be re-enabled (obsolete)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: WebSQLInThirdPartyContextEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: WebSQLInThirdPartyContextEnabled
- Example value:

```
<true/>
```

Back to top

WebSQLNonSecureContextEnabled

Force WebSQL in non-secure contexts to be enabled (deprecated)

> DEPRECATED: This policy is deprecated. It is currently supported but will become obsolete in a future release.

Supported versions:

- On Windows and macOS since 107, until 110

Description

This policy is deprecated because it is a temporary policy to support WebSQL in non-secure contexts. It won't work in Microsoft Edge as soon as version 110. If you enable this policy, WebSQL in non-secure contexts will be enabled. If you disable or don't configure this policy, WebSQL in non-secure contexts will follow the default settings of the broser.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WebSQLNonSecureContextEnabled
- GP name: Force WebSQL in non-secure contexts to be enabled (deprecated)
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: WebSQLNonSecureContextEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: WebSQLNonSecureContextEnabled
- Example value:

```
<true/>
```

Back to top

WebSelectEnabled

Web Select Enabled

Supported versions:

- On Windows and macOS since 107 or later

Description

Web select lets users select and copy web content while preserving its formatting when pasted in most cases. It also allows more targeted selection on some web elements, such as copying a single column in a table.

If you enable or don't configure this policy, Web select is available through the right click context menu and the CTRL+SHIFT+X keyboard shortcut.

If you disable this policy, Web select won't be available.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WebSelectEnabled
- GP name: Web Select Enabled
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: WebSelectEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Mac information and settings

- Preference Key Name: WebSelectEnabled
- Example value:

```
<true/>
```

Back to top

WebWidgetAllowed

Enable the Edge bar

Supported versions:

- On Windows since 88 or later

Description

Enables the Edge bar. When enabled, users can use the Edge bar to search the web from their desktop or from an application. The Edge bar provides a search box that shows web suggestions and opens all web searches in Microsoft Edge. The search box provides search (powered by Bing) and URL suggestions. The Edge bar also includes feed tiles that users can click to see more information on msn.com in a new Microsoft Edge browser tab or window. The feed tiles may include ads. The Edge bar can be launched from the Microsoft Edge settings or from the "More tools" menu in Microsoft Edge.

If you enable or don't configure this policy: The Edge bar will be automatically enabled for all profiles. In the Microsoft Edge settings, users will see option to launch the Edge bar. In the Microsoft Edge settings, users will see the menu item to run the Edge bar at Windows startup (auto-start). The option to enable the Edge bar at startup will be toggled on if the WebWidgetIsEnabledOnStartup policy is enabled. If the WebWidgetIsEnabledOnStartup is disabled or not configured, the option to enable the Edge bar at startup will be toggled off. Users will see the menu item to launch the Edge bar from the Microsoft Edge "More tools" menu. Users can launch the Edge bar from "More tools". The Edge bar can be turned off by the "Quit" option in the

System tray or by closing the Edge bar from the taskbar. The Edge bar will be restarted on system reboot if auto-start is enabled.

If you disable this policy: The Edge bar will be disabled for all profiles. The option to launch the Edge bar from Microsoft Edge Settings will be disabled. The option to launch start the Edge bar at Windows startup (auto-start) will be disabled. The option to launch the Edge bar from Microsoft Edge "More tools" menu will be disabled.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WebWidgetAllowed
- GP name: Enable the Edge bar
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: WebWidgetAllowed
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

WebWidgetIsEnabledOnStartup

Allow the Edge bar at Windows startup

Supported versions:

- On Windows since 88 or later

Description

Allows the Edge bar to start running at Windows startup.

If you enable: The Edge bar will start running at Windows startup by default. If the Edge bar is disabled via WebWidgetAllowed policy, this policy will not start the Edge bar on Windows startup.

If you disable this policy: The Edge bar will not start at Windows startup for all profiles. The option to start the Edge bar at Windows startup will be disabled and toggled off in Microsoft Edge settings.

If you don't configure the policy: The Edge bar will not start at Windows startup for all profiles. The option to start the Edge bar at Windows startup will be toggled off in Microsoft Edge settings.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WebWidgetIsEnabledOnStartup
- GP name: Allow the Edge bar at Windows startup
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: WebWidgetIsEnabledOnStartup
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

WinHttpProxyResolverEnabled

Use Windows proxy resolver

Supported versions:

- On Windows since 84 or later

Description

This policy will be superseded by a similar feature in a future release. For more information, see https://crbug.com/1032820.

Use Windows to resolve proxies for all browser networking instead of the proxy resolver built into Microsoft Edge. The Windows proxy resolver enables Windows proxy features such as DirectAccess/NRPT.

This policy comes with the problems described by https://crbug.com/644030. It causes PAC files to be fetched and executed by Windows code, including PAC files set via the ProxyPacUrl policy. Since Network Fetches for the PAC file happen via Windows instead of Microsoft Edge code, network policies such as DnsOverHttpsMode will not apply to network fetches for a PAC file.

If you enable this policy, the Windows proxy resolver will be used.

If you disable or don't configure this policy, the Microsoft Edge proxy resolver will be used.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: No - Requires browser restart

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WinHttpProxyResolverEnabled
- GP name: Use Windows proxy resolver
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A

- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: WinHttpProxyResolverEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

WindowOcclusionEnabled

Enable Window Occlusion

Supported versions:

- On Windows since 89 or later

Description

Enables window occlusion in Microsoft Edge.

If you enable this setting, to reduce CPU and power consumption Microsoft Edge will detect when a window is covered by other windows, and will suspend work painting pixels.

If you disable this setting Microsoft Edge will not detect when a window is covered by other windows.

If this policy is left not set, window hiding detection will be enabled.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Boolean

Windows information and settings

Group Policy (ADMX) info

- GP unique name: WindowOcclusionEnabled
- GP name: Enable Window Occlusion
- GP path (Mandatory): Administrative Templates/Microsoft Edge/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdge.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge
- Path (Recommended): N/A
- Value Name: WindowOcclusionEnabled
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

See also

- Configuring Microsoft Edge
- Microsoft Edge Enterprise landing page
- Microsoft Security Baselines Blog

Microsoft Edge - Update policies

11/1/2022 • 18 minutes to read • Edit Online

The latest version of Microsoft Edge includes the following policies that you can use to control how and when Microsoft Edge is updated.

For information about other policies available in Microsoft Edge, check out Microsoft Edge browser policy reference

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

Available policies

These tables list all of the update-related group policies available in this release of Microsoft Edge. Use the links in the table to get more details about specific policies.

- Applications
- Preferences
- Proxy Server
- Microsoft Edge Update
- Microsoft Edge WebView

Applications

POLICY NAME	CAPTION
InstallDefault	Allow installation default
UpdateDefault	Update policy override default
Install	Allow installation (per channel)
Update	Update policy override (per channel)
Allowsxs	Allow Microsoft Edge Side by Side browser experience
CreateDesktopShortcutDefault	Prevent Desktop Shortcut creation upon install default
CreateDesktopShortcut	Prevent Desktop Shortcut creation upon install (per channel)
RollbackToTargetVersion	Rollback to Target version (per channel)
TargetVersionPrefix	Target version override (per channel)
TargetChannel	Target Channel override (per channel)

Preferences

POLICY NAME	CAPTION
AutoUpdateCheckPeriodMinutes	Microsoft AutoUpdate check period override
UpdatesSuppressed	Time period in each day to suppress Microsoft AutoUpdate check

Proxy Server

POLICY NAME	CAPTION
ProxyMode	Choose how to specify a proxy server settings
ProxyPacUrl	URL to proxy .pac file
ProxyServer	Address or URL of a proxy server

Microsoft Edge Update

POLICY NAME	CAPTION
UpdaterExperimentationAndConfigurationServiceControl	Control updater's communication with the Experimentation and Configuration Service

Microsoft Edge WebView

POLICY NAME	CAPTION
Install	Allow installation
Update	Update policy override

Applications policies

Back to top

InstallDefault

Allow installation default

> Microsoft Edge Update 1.2.145.5 and later

Description

You can specify the default behavior of all channels to allow or block Microsoft Edge on domain-joined devices.

You can override this policy for individual channels by enabling the 'Allow installation' policy for specific channels.

If you disable this policy, the installation of Microsoft Edge is blocked. This only affects the installation of Microsoft Edge software when the 'Allow installation' policy is set to Not Configured.

This policy doesn't prevent Microsoft Edge Update from running or prevent users from installing Microsoft Edge software using other methods.

This policy is available only on Windows instances that are joined to a Microsoft® Active Directory® domain.

Windows information and settings

Group Policy (ADMX) info

- GP unique name: InstallDefault
- GP name: Allow installation default
- GP path: Administrative Templates/Microsoft Edge Update/Applications
- GP ADMX file name: msedgeupdate.admx

Windows Registry Settings

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EdgeUpdate
- Value Name: InstallDefault
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

UpdateDefault

Update policy override default

> Microsoft Edge Update 1.2.145.5 and later

Description

Lets you specify the default behavior for all channels concerning the way Microsoft Edge Update handles available updates for Microsoft Edge. Can be overridden for individual channels by specifying the 'Update policy override' policy for those specific channels.

If you enable this policy, Microsoft Edge Update handles Microsoft Edge updates according to how you configure the following options:

- Always allow updates: Updates are always applied when found, either by periodic update check or by a manual update check.
- Automatic silent updates only: Updates are applied only when they're found by the periodic update check.
- Manual updates only: Updates are applied only when the user runs a manual update check.
- Updates disabled: Updates are never applied.

If you select manual updates, make sure you periodically check for updates by using the app's manual update mechanism, if available. If you disable updates, periodically check for updates, and distribute them to users.

If you don't enable and configure this policy, Microsoft Edge Update handles available updates as specified by the 'Update policy override' policy.

This policy is available only on Windows instances that are joined to a Microsoft® Active Directory® domain.

Windows information and settings

Group Policy (ADMX) info

- GP unique name: UpdateDefault
- GP name: Update policy override default
- GP path: Administrative Templates/Microsoft Edge Update/Applications
- GP ADMX file name: msedgeupdate.admx

Windows Registry Settings

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EdgeUpdate
- Value Name: UpdateDefault
- Value Type: REG_DWORD

Example value:

```
0x00000003
```

Back to top

Install

Allow installation

> Microsoft Edge Update 1.2.145.5 and later

Description

Specifies whether a Microsoft Edge channel can be installed on domain-joined devices.

If you enable this policy for a channel, Microsoft Edge will not be blocked from installation.

If you disable this policy for a channel, Microsoft Edge will be blocked from installation.

If you don't configure this policy for a channel, the 'Allow installation default' policy configuration determines whether users can install that channel of Microsoft Edge.

This policy is available only on Windows instances that are joined to a Microsoft® Active Directory® domain.

Windows information and settings

Group Policy (ADMX) info

- GP unique name: Install
- GP name: Allow installation
- GP path:
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge Beta
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge Canary
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge Dev
- GP ADMX file name: msedgeupdate.admx

Windows Registry Settings

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EdgeUpdate
- Value Name:
  - (Stable): Install{56EB18F8-B008-4CBD-B6D2-8C97FE7E9062}
  - (Beta): Install{2CD8A007-E189-409D-A2C8-9AF4EF3C72AA}
  - (Canary): Install{65C35B14-6C1D-4122-AC46-7148CC9D6497}
  - (Dev): Install{0D50BFEC-CD6A-4F9A-964C-C7416E3ACB10}
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

Update

Update policy override

> Microsoft Edge Update 1.2.145.5 and later

Description

Specifies how Microsoft Edge Update handles available updates from Microsoft Edge.

If you enable this policy, Microsoft Edge Update handles Microsoft Edge updates according to how you configure the following options:

- Always allow updates: Updates are always applied when found, either by periodic update check or by a manual update check.
- Automatic silent updates only: Updates are applied only when they're found by the periodic update check.
- Manual updates only: Updates are applied only when the user runs a manual update check. (Not all apps provide an interface for this option.)
- Updates disabled: Updates are never applied.

If you select manual updates, make sure you periodically check for updates by using the app's manual update mechanism, if available. If you disable updates, periodically check for updates, and distribute them to users.

If you don't enable and configure this policy, Microsoft Edge Update handles available updates as specified by the 'Update policy override default' policy.

For more information, see https://go.microsoft.com/fwlink/?linkid=2136406.

This policy is available only on Windows instances that are joined to a Microsoft® Active Directory® domain.

Windows information and settings

Group Policy (ADMX) info

- GP unique name: Update
- GP name: Update policy override
- GP path:
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge Beta
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge Canary
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge Dev
- GP ADMX file name: msedgeupdate.admx

Windows Registry Settings

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EdgeUpdate
- Value Name:
  - (Stable): Update{56EB18F8-B008-4CBD-B6D2-8C97FE7E9062}
  - (Beta): Update{2CD8A007-E189-409D-A2C8-9AF4EF3C72AA}
  - (Canary): Update{65C35B14-6C1D-4122-AC46-7148CC9D6497}
  - (Dev): Update{0D50BFEC-CD6A-4F9A-964C-C7416E3ACB10}
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

Allowsxs

Allow Microsoft Edge Side by Side browser experience

> Microsoft Edge Update 1.2.145.5 and later

Description

This policy lets a user run Microsoft Edge (Edge HTML) and Microsoft Edge (Chromium-based) side by side.

If this policy is set to “Not configured”, Microsoft Edge (Chromium-based) will replace Microsoft Edge (Edge

HTML) after the Microsoft Edge (Chromium-based) stable channel and the November 2019 security updates are installed. This is the same behavior as the "Disabled" setting.

The "Disabled" setting blocks a side-by-side experience and Microsoft Edge (Chromium-based) will replace Microsoft Edge (Edge HTML) after the Microsoft Edge (Chromium-based) stable channel and the November 2019 security updates are installed. This is the same behavior as the "Not Configured" setting.

When this policy is "Enabled", Microsoft Edge (Chromium-based) and Microsoft Edge (Edge HTML) can run side by side after Microsoft Edge (Chromium-based) is installed.

For this group policy to take effect, it must be configured before the automatic install of Microsoft Edge (Chromium-based) by Windows Update. Note: A user can block the automatic update of Microsoft Edge (Chromium-based) by using the Microsoft Edge (Chromium-based) Blocker Toolkit.

Starting with Windows 10 version 20H2 Microsoft Edge Legacy and the side-by-side browser experience are not supported.

Windows information and settings

Group Policy (ADMX) info

- GP unique name: Allowsxs
- GP name: Allow Microsoft Edge Side by Side browser experience
- GP path: Administrative Templates/Microsoft Edge Update/Applications
- GP ADMX file name: msedgeupdate.admx

Windows Registry Settings

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EdgeUpdate
- Value Name: Allowsxs
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

CreateDesktopShortcutDefault

Prevent Desktop Shortcut creation upon install default

> Microsoft Edge Update 1.3.128.0 and later

Description

Lets you specify the default behavior for all channels for creating a desktop shortcut when Microsoft Edge is installed.

If you enable this policy a desktop shortcut is created when Microsoft Edge is installed. If you disable this policy, no desktop shortcut will be created when Microsoft Edge is installed. If you don't configure this policy a desktop shortcut to Microsoft Edge will be created during installation. If Microsoft Edge is already installed, this policy will have no effect.

Windows information and settings

Group Policy (ADMX) info

- GP unique name: CreateDesktopShortcutDefault
- GP name: Prevent Desktop Shortcut creation upon install default
- GP path: Administrative Templates/Microsoft Edge Update/Applications
- GP ADMX file name: msedgeupdate.admx

Windows Registry Settings

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EdgeUpdate

- Value Name: CreateDesktopShortcutDefault
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

CreateDesktopShortcut

Prevent Desktop Shortcut creation upon install

> Microsoft Edge Update 1.3.128.0 and later

Description

If you enable this policy a desktop shortcut is created when Microsoft Edge is installed. If you disable this policy, no desktop shortcut will be created when Microsoft Edge is installed. If you don't configure this policy a desktop shortcut to Microsoft Edge will be created during installation. If Microsoft Edge is already installed, this policy will have no effect.

If you don't configure this policy for a channel, the 'Prevent Desktop Shortcut creation upon install default' policy configuration determines shortcut creation when Microsoft Edge is installed.

Windows information and settings

Group Policy (ADMX) info

- GP unique name: CreateDesktopShortcut
- GP name: Prevent Desktop Shortcut creation upon install
- GP path:
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge Beta
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge Canary
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge Dev
- GP ADMX file name: msedgeupdate.admx

Windows Registry Settings

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EdgeUpdate
- Value Name:
  - (Stable): CreateDesktopShortcut{56EB18F8-B008-4CBD-B6D2-8C97FE7E9062}
  - (Beta): CreateDesktopShortcut{2CD8A007-E189-409D-A2C8-9AF4EF3C72AA}
  - (Canary): CreateDesktopShortcut{65C35B14-6C1D-4122-AC46-7148CC9D6497}
  - (Dev): CreateDesktopShortcut{0D50BFEC-CD6A-4F9A-964C-C7416E3ACB10}
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

RollbackToTargetVersion

Rollback to Target version

> Microsoft Edge Update 1.3.133.3 and later

Description

Specifies that Microsoft Edge Update should rollback installations of Microsoft Edge to the version indicated in 'Target version override'.

This policy has no effect unless 'Target version override' is set and 'Update policy override' is set to one of the ON states (Always allow updates, Automatic silent updates only, Manual updates only).

If you disable this policy or don't configure it, installs that have a version higher than that specified by 'Target version override' will be left as-is.

If you enable this policy, installs that have a current version higher than specified by the 'Target version override' will be downgraded to the target version.

We recommend that users install the latest version of the Microsoft Edge browser to ensure protection by the latest security updates. Rollback to an earlier version risks exposure to known security issues. This policy is meant to be used as a temporary fix to address issues in a Microsoft Edge browser update.

Before temporarily rolling back your browser version, we recommend that you turn on Sync (https://go.microsoft.com/fwlink/?linkid=2133032) for all users in your organization. If you don't turn on Sync, there is a risk of permanent browsing data loss. Use this policy at your own risk.

Note: All versions available for rollback can be viewed here EdgeEnterprise.

This policy applies to Microsoft Edge version 86 or later.

See Edge support for WIP for more information.

This policy is available only on Windows instances that are joined to a Microsoft® Active Directory® domain.

Windows information and settings

Group Policy (ADMX) info

- GP unique name: RollbackToTargetVersion
- GP name: Rollback to Target version
- GP path:
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge Beta
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge Canary
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge Dev
- GP ADMX file name: msedgeupdate.admx

Windows Registry Settings

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EdgeUpdate
- Value Name:
  - (Stable): RollbackToTargetVersion{56EB18F8-B008-4CBD-B6D2-8C97FE7E9062}
  - (Beta): RollbackToTargetVersion{2CD8A007-E189-409D-A2C8-9AF4EF3C72AA}
  - (Canary): RollbackToTargetVersion{65C35B14-6C1D-4122-AC46-7148CC9D6497}
  - (Dev): RollbackToTargetVersion{0D50BFEC-CD6A-4F9A-964C-C7416E3ACB10}
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

TargetVersionPrefix

Target version override

> Microsoft Edge Update 1.3.119.43 and later

Description

When this policy is enabled, and auto-update is enabled, Microsoft Edge will be updated to the version specified by this policy value.

The policy value must be a specific Microsoft Edge version, for example, 83.0.499.12.

If a device has newer version of Microsoft Edge than the value specified, Microsoft Edge will remain on the newer version and not downgrade to the specified version.

If the specified version does not exist, or is improperly formatted, then Microsoft Edge will remain on its current version and not update to future versions automatically.

For more information, see https://go.microsoft.com/fwlink/?linkid=2136707.

This policy is available only on Windows instances that are joined to a Microsoft® Active Directory® domain.

Windows information and settings

Group Policy (ADMX) info

- GP unique name: TargetVersionPrefix
- GP name: Target version override
- GP path:
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge Beta
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge Canary
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge Dev
- GP ADMX file name: msedgeupdate.admx

Windows Registry Settings

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EdgeUpdate
- Value Name:
  - (Stable): TargetVersionPrefix{56EB18F8-B008-4CBD-B6D2-8C97FE7E9062}
  - (Beta): TargetVersionPrefix{2CD8A007-E189-409D-A2C8-9AF4EF3C72AA}
  - (Canary): TargetVersionPrefix{65C35B14-6C1D-4122-AC46-7148CC9D6497}
  - (Dev): TargetVersionPrefix{0D50BFEC-CD6A-4F9A-964C-C7416E3ACB10}
- Value Type: REG_SZ

Example value:

```
83.0.499.12
```

Back to top

TargetChannel

Target Channel override

> Microsoft Edge Update 1.3.147.1 and later

Description

Specifies which Channel Microsoft Edge should be updated to.

If you enable this policy, the Microsoft Edge will be updated to the Channel according to how you configure the following options:

- Stable: Microsoft Edge will be updated to the latest stable version.

- Beta: Microsoft Edge will be updated to the latest beta version.
- Dev: Microsoft Edge will be updated to the latest dev version.
- Extended Stable: Microsoft Edge will be updated to the latest extended stable version, which follows a longer release cadence than stable. For more information, visit https://go.microsoft.com/fwlink/?linkid=2163508.

If you do not configure this policy, Microsoft Edge will be updated to the latest version available for the default Channel.

This policy is available only on Windows instances that are joined to a Microsoft® Active Directory® domain.

Windows information and settings

Group Policy (ADMX) info

- GP unique name: TargetChannel
- GP name: Target Channel override
- GP path:
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge Beta
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge Canary
  - Administrative Templates/Microsoft Edge Update/Applications/Microsoft Edge Dev
- GP ADMX file name: msedgeupdate.admx

Windows Registry Settings

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EdgeUpdate
- Value Name:
  - (Stable): TargetChannel{56EB18F8-B008-4CBD-B6D2-8C97FE7E9062}
  - (Beta): TargetChannel{2CD8A007-E189-409D-A2C8-9AF4EF3C72AA}
  - (Canary): TargetChannel{65C35B14-6C1D-4122-AC46-7148CC9D6497}
  - (Dev): TargetChannel{0D50BFEC-CD6A-4F9A-964C-C7416E3ACB10}
- Value Type: REG_SZ

Example value:

```
dev
```

Back to top

Preferences policies

Back to top

AutoUpdateCheckPeriodMinutes

Auto-update check period override

> Microsoft Edge Update 1.2.145.5 and later

Description

Minimum number of minutes between automatic update checks.

Set this policy to the value 0 to disable all periodic network traffic by Microsoft Edge Update. This is not recommended, as it prevents Microsoft Edge Update itself from receiving stability and security updates.

The 'Update policy override default' and per-application 'Update policy override' settings should be used to manage application updates rather than this setting.

Windows information and settings

Group Policy (ADMX) info

- GP unique name: AutoUpdateCheckPeriodMinutes
- GP name: Auto-update check period override
- GP path: Administrative Templates/Microsoft Edge Update/Preferences
- GP ADMX file name: msedgeupdate.admx

Windows Registry Settings

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EdgeUpdate
- Value Name: AutoUpdateCheckPeriodMinutes
- Value Type: REG_DWORD

Example value:

```
0x00000578
```

Back to top

UpdatesSuppressed

Time period in each day to suppress auto-update check

> Microsoft Edge Update 1.3.33.5 and later

Description

If you enable this policy, update checks are suppressed each day starting at Hour:Minute for Duration (in minutes). Duration isn't affected by daylight saving time. For example, if the start time is 22:00 and the duration is 480 minutes, updates will be suppressed for exactly 8 hours, regardless of whether daylight saving time starts or ends during this period.

If you disable or don't configure this policy, update checks aren't suppressed during any specific period.

Windows information and settings

Group Policy (ADMX) info

- GP unique name: UpdatesSuppressed
- GP name: Time period in each day to suppress auto-update check
  - Options { Hour, Minute, Duration }
- GP path: Administrative Templates/Microsoft Edge Update/Preferences
- GP ADMX file name: msedgeupdate.admx

Windows Registry Settings

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EdgeUpdate
- Value Name:
  - UpdatesSuppressedDurationMin
  - UpdatesSuppressedStartHour
  - UpdatesSuppressedStartMin
- Value Type: REG_DWORD

Example value:

```
duration   : 0x0000003c
start hour : 0x00000001
start min  : 0x00000002
```

Back to top

Proxy Server policies

Back to top

ProxyMode

Choose how to specify a proxy server setting

> Microsoft Edge Update 1.3.21.81 and later

Description

Allows you to specify the proxy server settings that are used by Microsoft Edge Update.

If you enable this policy, you can choose between the following proxy server options:

- If you choose to never use a proxy server and always connect directly, all other options are ignored.
- If you choose to use system proxy settings or autodetect the proxy server, all other options are ignored.
- If you choose fixed server proxy mode, you can specify further options in 'Address or URL of a proxy server' policy.
- If you choose to use a .pac proxy script, you must specify the URL for the script in 'URL to proxy .pac file' policy.

If you enable this policy, users in your organization can't change the proxy settings in Microsoft Edge Update.

If you disable or don't configure this policy, no proxy server settings are configured, but users in your organization can choose their own proxy settings for Microsoft Edge Update.

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ProxyMode
- GP name: Choose how to specify a proxy server setting
- GP path: Administrative Templates/Microsoft Edge Update/Proxy Server
- GP ADMX file name: msedgeupdate.admx

Windows Registry Settings

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EdgeUpdate
- Value Name: ProxyMode
- Value Type: REG_SZ

Example value:

```
fixed_servers
```

Back to top

ProxyPacUrl

URL to proxy .pac file

> Microsoft Edge Update 1.3.21.81 and later

Description

Allows you to specify a URL for a proxy auto-config (PAC) file.

If you enable this policy, you can specify a URL for a PAC file to automate how Microsoft Edge Update selects the appropriate proxy server for fetching a particular website.

This policy is applied only if you have specified manual proxy settings in the 'Choose how to specify a proxy server settings' policy.

Don't configure this policy if you have selected a proxy setting other than manual in the 'Choose how to specify

a proxy server settings' policy.

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ProxyPacUrl
- GP name: URL to proxy .pac file
- GP path: Administrative Templates/Microsoft Edge Update/Proxy Server
- GP ADMX file name: msedgeupdate.admx

Windows Registry Settings

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EdgeUpdate
- Value Name: ProxyPacUrl
- Value Type: REG_SZ

Example value:

```
https://www.microsoft.com
```

Back to top

ProxyServer

Address or URL of a proxy server

> Microsoft Edge Update 1.3.21.81 and later

Description

Allows you to specify the URL of the proxy server for Microsoft Edge Update to use.

If you enable this policy, you can set the proxy server URL used by Microsoft Edge Update in your organization.

This policy is applied only if you have selected manual proxy settings in the 'Choose how to specify a proxy server settings' policy.

Don't configure this policy if you have selected a proxy setting other than manual in the 'Choose how to specify a proxy server settings' policy.

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ProxyServer
- GP name: Address or URL of a proxy server
- GP path: Administrative Templates/Microsoft Edge Update/Proxy Server
- GP ADMX file name: msedgeupdate.admx

Windows Registry Settings

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EdgeUpdate
- Value Name: ProxyServer
- Value Type: REG_SZ

Example value:

```
https://www.microsoft.com
```

Back to top

Microsoft Edge Update policies

Back to top

UpdaterExperimentationAndConfigurationServiceControl

Control updater's communication with the Experimentation and Configuration Service

> Microsoft Edge Update 1.3.145.1 and later

Description

In Microsoft Edge Update, the Experimentation and Configuration Service is used to deploy experimentation payload.

Experimentation payload consists of a list of early in development features that Microsoft is enabling for testing and feedback.

If you enable this policy, experimentation payload is downloaded from the Experimentation and Configuration Service.

If you disable this policy, communication with the Experimentation and Configuration Service is stopped completely.

If you don't configure this policy, on a managed device the behavior is same as policy 'disabled'.

If you don't configure this policy, on an unmanaged device the behavior is same as policy 'enabled'.

Windows information and settings

Group Policy (ADMX) info

- GP unique name: UpdaterExperimentationAndConfigurationServiceControl
- GP name: Control updater's communication with the Experimentation and Configuration Service
- GP path: Administrative Templates/Microsoft Edge Update/Microsoft Edge Update
- GP ADMX file name: msedgeupdate.admx

Windows Registry Settings

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EdgeUpdate
- Value Name: UpdaterExperimentationAndConfigurationServiceControl
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

Microsoft Edge WebView policies

Back to top

Install (WebView)

Allow installation

> Microsoft Edge Update 1.3.127.1 and later

Description

Lets you specify whether Microsoft Edge WebView can be installed using Microsoft Edge Update.

- If you enable this policy, users can install Microsoft Edge WebView through Microsoft Edge Update.
- If you disable this policy, users cannot install Microsoft Edge WebView through Microsoft Edge Update.
- If you don't configure this policy, the 'Allow installation default' policy configuration determines whether users can install Microsoft Edge WebView through Microsoft Edge Update.

Windows information and settings

Group Policy (ADMX) info

- GP unique name: Install
- GP name: Allow installation
- GP path: Administrative Templates/Microsoft Edge Update/Microsoft Edge WebView
- GP ADMX file name: msedgeupdate.admx

Windows Registry Settings

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EdgeUpdate
- Value Name:
  - Install{F3017226-FE2A-4295-8BDF-00C3A9A7E4C5}
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

Update (WebView)

Update policy override

> Microsoft Edge Update 1.3.127.1 and later

Description

Lets you specify whether or not automatic updates are enabled for Microsoft Edge WebView. Microsoft Edge WebView is a component used by applications to display web content. Automatic updates are enabled by default. Disabling automatic updates for Microsoft Edge WebView might cause compatibility issues with applications that depend on this component.

If you enable this policy, Microsoft Edge Update handles Microsoft Edge WebView updates according to how you configure the following options:

- Always allow updates: Updates are automatically downloaded and applied
- Updates disabled: Updates are never downloaded or applied

If you don't enable this policy, updates are automatically downloaded and applied.

Windows information and settings

Group Policy (ADMX) info

- GP unique name: Update
- GP name: Update policy override
- GP path: Administrative Templates/Microsoft Edge Update/Microsoft Edge WebView
- GP ADMX file name: msedgeupdate.admx

Windows Registry Settings

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\EdgeUpdate
- Value Name:
  - Update{F3017226-FE2A-4295-8BDF-00C3A9A7E4C5}
- Value Type: REG_DWORD

Example value:

```
0x00000001
```

Back to top

See also

- Configuring Microsoft Edge
- Microsoft Edge Enterprise landing page

Microsoft Edge WebView2 - Policies

11/1/2022 • 4 minutes to read • Edit Online

The latest version of Microsoft Edge WebView2 includes the following policies. You can use these policies to configure how Microsoft Edge WebView2 runs in your organization.

For information about an additional set of policies used to control how and when Microsoft Edge WebView2 is updated, check out Microsoft Edge update policy reference.

> **NOTE**
> This article applies to Microsoft Edge version 87 or later.

Available policies

These tables list all of the group policies available in this release of Microsoft Edge WebView2. Use the links in the table to get more details about specific policies.

- Loader Override Settings
- Additional

Loader Override Settings

POLICY NAME	CAPTION
BrowserExecutableFolder	Configure the location of the browser executable folder
ReleaseChannelPreference	Set the release channel search order preference

Additional

POLICY NAME	CAPTION
ExperimentationAndConfigurationServiceControl	Control communication with the Experimentation and Configuration Service

Loader Override Settings policies

Back to top

BrowserExecutableFolder

Configure the location of the browser executable folder

Supported versions:

- On Windows since 87 or later

Description

This policy configures WebView2 applications to use the WebView2 Runtime in the specified path. The folder should contain the following files: msedgewebview2.exe, msedge.dll, and so on.

To set the value for the folder path, provide a Value name and Value pair. Set value name to the Application User Model ID or the executable file name. You can use the "*" wildcard as value name to apply to all applications.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: BrowserExecutableFolder
- GP name: Configure the location of the browser executable folder
- GP path (Mandatory): Administrative Templates/Microsoft Edge WebView2/Loader Override Settings
- GP path (Recommended): N/A
- GP ADMX file name: MSEdgeWebView2.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\WebView2\BrowserExecutableFolder
- Path (Recommended): N/A
- Value Name: list of REG_SZ
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\WebView2\BrowserExecutableFolder = "Name: *, Value: C:\\Program
Files\\Microsoft Edge WebView2 Runtime Redistributable 85.0.541.0 x64"
```

Back to top

ReleaseChannelPreference

Set the release channel search order preference

Supported versions:

- On Windows since 87 or later

Description

The default channel search order is WebView2 Runtime, Beta, Dev, and Canary.

To reverse the default search order, set this policy to 1.

To set the value for the release channel preference, provide a Value name and Value pair. Set value name to the Application User Model ID or the executable file name. You can use the "*" wildcard as value name to apply to all applications.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- List of strings

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ReleaseChannelPreference
- GP name: Set the release channel search order preference
- GP path (Mandatory): Administrative Templates/Microsoft Edge WebView2/Loader Override Settings

- GP path (Recommended): N/A
- GP ADMX file name: MSEdgeWebView2.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\WebView2\ReleaseChannelPreference
- Path (Recommended): N/A
- Value Name: list of REG_SZ
- Value Type: list of REG_SZ

Example value:

```
SOFTWARE\Policies\Microsoft\Edge\WebView2\ReleaseChannelPreference = "Name: *, Value: 1"
```

Back to top

Additional policies

Back to top

ExperimentationAndConfigurationServiceControl

Control communication with the Experimentation and Configuration Service

Supported versions:

- On Windows since 97 or later

Description

The Experimentation and Configuration Service is used to deploy Experimentation and Configuration payloads to the client.

Experimentation payload consists of a list of early in development features that Microsoft is enabling for testing and feedback.

Configuration payload consists of a list of recommended settings that Microsoft wants to deploy to optimize the user experience.

Configuration payload may also contain a list of actions to take on certain domains for compatibility reasons. For example, the browser may override the User Agent string on a website if that website is broken. Each of these actions is intended to be temporary while Microsoft tries to resolve the issue with the site owner.

If you set this policy to 'FullMode', the full payload is downloaded from the Experimentation and Configuration Service. This includes both the experimentation and configuration payloads.

If you set this policy to 'ConfigurationsOnlyMode', only the configuration payload is downloaded.

If you set this policy to 'RestrictedMode', the communication with the Experimentation and Configuration Service is stopped completely. Microsoft does not recommend this setting.

If you don't configure this policy on a managed device, the behavior on Beta and Stable channels is the same as the 'ConfigurationsOnlyMode'. On Canary and Dev channels the behavior is the same as 'FullMode'.

If you don't configure this policy on an unmanaged device, the behavior is the same as the 'FullMode'.

Policy options mapping:

- FullMode (2) = Retrieve configurations and experiments
- ConfigurationsOnlyMode (1) = Retrieve configurations only
- RestrictedMode (0) = Disable communication with the Experimentation and Configuration Service

Use the preceding information when configuring this policy.

Supported features:

- Can be mandatory: Yes
- Can be recommended: No
- Dynamic Policy Refresh: Yes

Data Type:

- Integer

Windows information and settings

Group Policy (ADMX) info

- GP unique name: ExperimentationAndConfigurationServiceControl
- GP name: Control communication with the Experimentation and Configuration Service
- GP path (Mandatory): Administrative Templates/Microsoft Edge WebView2/
- GP path (Recommended): N/A
- GP ADMX file name: MSEdgeWebView2.admx

Windows Registry Settings

- Path (Mandatory): SOFTWARE\Policies\Microsoft\Edge\WebView2
- Path (Recommended): N/A
- Value Name: ExperimentationAndConfigurationServiceControl
- Value Type: REG_DWORD

Example value:

```
0x00000002
```

Back to top

See also

- Configuring Microsoft Edge
- Microsoft Edge Enterprise landing page
- Microsoft Security Baselines Blog

Backwards compatibility for the Enterprise New tab page

11/1/2022 • 2 minutes to read • Edit Online

This article describes the change to the New tab page and how users can be backwards compatible with Microsoft Edge version 87 and earlier.

> **NOTE**
> This article applies to Microsoft Edge version 87 or later.

Information feeds from single endpoint

The new version of the Enterprise New tab page combines compliant Microsoft 365 content with industry relevant and compliant information feeds that are served via the MSN.com endpoint.

> **NOTE**
> Office 365 content was originally served using the Office.com domain.

If access to the MSN.com domain is restricted for your organization, we strongly recommend giving users access to this https://ntp.msn.com.

If you need more time to enable access to the MSN domain, we recommend using the NewTabPageSetFeedType, that lets you choose either the Microsoft News or Office 365 feed experience for the new tab page.

Keep using Office.com

You can configure the **NewTabPageSetFeedType** policy to keep using the deprecated Office.com domain.

> **IMPORTANT**
> The **NewTabPageSetFeedType** policy and the Office.com domain that serves Office 365 content will quit working when Microsoft Edge version 90 is released.

The following policy settings will force the Enterprise New tab page to render Office document content from the Office.com domain.

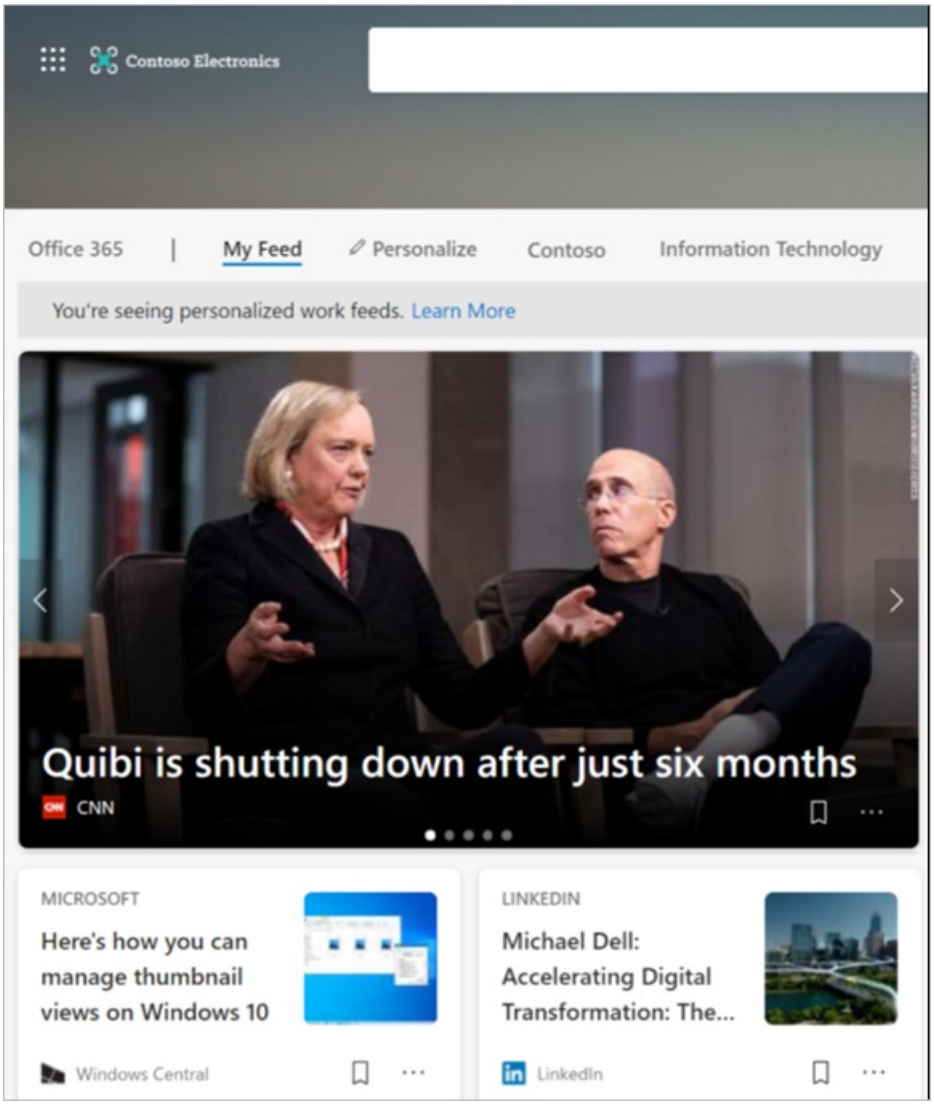
- Set the policy as **Mandatory**.
- Set the value of the policy mapping to **Office (1) = Office 365 feed experience**.

If the switch to the Office.com isn't possible, reach out and send us feedback. Another option is to configure the NewTabPageLocation so it points to an endpoint URL that's allowed by your organization.

> **NOTE**
> The **NewTabPageLocation** policy has precedence if the **NewTabPageSetFeedType** policy is also configured.

Enterprise users will now get Microsoft news content via My Feed

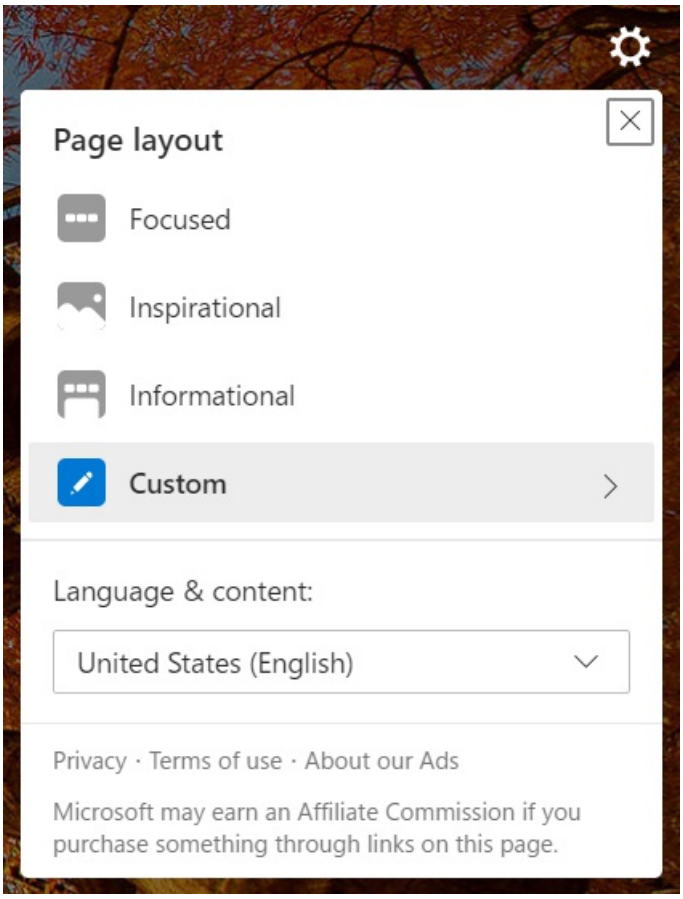
The Enterprise New tab page will offer industry relevant information in **My Feed** and Office 365 content in a single view for users signed in with their Azure Active Directory (Azure AD) account. For users signed in with their Azure Active Directory (Azure AD) who selected the Microsoft News option in the settings flyout, their new tab page view will be replaced with **My Feed** content. When they open a new tab page in the browser it will look like the example in the next screenshot.



> **NOTE**
>
> Users who aren't signed in with Azure AD will continue to see the MSN News feed when they open a new tab.

Page layout

With the changes to the New tab page, the Page layout no longer has to control two specific content types (Office 365 and Microsoft News), so the content toggle isn't available. The next screenshot shows the flyout for the Page layout.


Page layout
Focused
Inspirational
Informational
Custom
Language & content:
United States (English)
Privacy · Terms of use · About our Ads
Microsoft may earn an Affiliate Commission if you purchase something through links on this page.

If you want to keep accessing Microsoft News content that isn't tied to your organization, you must use a different browser profile. Go to *edge://settings/profiles* and sign out of your Azure AD profile. This action will bring up the standard view for the Enterprise new tab page.

See also

- Microsoft Edge Enterprise landing page
- Enterprise Mode for Internet Explorer 11

Block access to consumer accounts

11/1/2022 • 2 minutes to read • Edit Online

You can prevent users from signing into Google services using any accounts other than the accounts you provided them with. Reasons for blocking access are to prevent users on your corporate network using their personal Gmail accounts, or accessing a managed Google account from another domain.

Users might see the following message when you block access to consumer accounts: "This account is not allowed to sign in within this network".

> **NOTE**
> This article applies to Microsoft Edge Stable version 104 or later.

What does this policy do?

This policy causes the **X-GoogApps-Allowed-Domains:** header to be appended to all HTTP and HTTPS requests to all google.com domains. This header is followed by a comma-separated list with the allowed domain names.

Example: `X-GoogApps-Allowed-Domains: mydomain1.com, mydomain2.com`

> **NOTE**
> Microsoft Edge, which is built on Chromium, is inheriting this upstream policy from the Chromium open source project.

Configure policy settings

To learn how to configure Microsoft Edge policy settings in Intune, see Configure Microsoft Edge policy settings with Microsoft Intune.

Content license

> **NOTE**
> Portions of this page are modifications based on work created and shared by Chromium.org and used according to terms described in the Creative Commons Attribution 4.0 International License. The original page can be found here.

This work is licensed under a Creative Commons Attribution 4.0 International License.

Understand the ClickOnce and DirectInvoke features in Microsoft Edge

11/1/2022 • 6 minutes to read • Edit Online

ClickOnce and DirectInvoke are features available in IE and Microsoft Edge that support the use of a file handler to download files from a website. Although they serve different purposes, both features let websites specify that a file requested for download is passed to a file handler on the user's device. ClickOnce requests are handled by the native file handler in Windows. DirectInvoke requests are handled by a registered file handler specified by the website hosting the file.

After setting up ClickOnce or DirectInvoke, the ClickOnce or DirectInvoke prompts can be bypassed by setting up other enterprise policies. These policies can support either bypassing the ClickOnce or DirectInvoke prompts for specified file types for all domains or for specified file types from specified domains.

For more information about these features, see:

- ClickOnce
- DirectInvoke

> **NOTE**
> Currently, Chromium doesn't provide native support for ClickOnce or DirectInvoke.

Overview: prerequisites and process

For ClickOnce and DirectInvoke to work as designed and for the file handler to be successfully requested, the file handler must be registered to the operating system as supporting ClickOnce or DirectInvoke. This registration typically happens when the original operating system is installed or when a new program that's installed requests the ability to use DirectInvoke for updates.

When a website receives a download request that requires ClickOnce or DirectInvoke, the following actions happen:

- The website requests that the browser use a specified file handler.
- The browser checks the operating system registry to see if the file handler is registered for the requested file type.
- If the file handler is registered, the browser calls the file handler and passes the URL as an argument to the file handler.
- The file handler processes the URL and downloads the file.

> **NOTE**
> The URL is used to determine the source of the file, as well as any parameters to use when accessing the file. For example: endpoints, a manifest, or metadata.

Use cases

The following use cases are representative.

You can use ClickOnce to easily deploy and update software on devices with minimal user interaction. Users can install and run a Windows application by clicking a link in a web page. If configured correctly, the ClickOnce application can install programs without having users set configurations for the installer. For example, file locations, what options to install, and so on.

DirectInvoke use cases depend on the intent of the website requesting DirectInvoke. For example, the collaborative file-editing feature of Microsoft Word. Instead of clicking a link and downloading the entire copy of a document you're working on with your colleagues, DirectInvoke lets you download the parts of the document that have been changed. This strategy reduces the amount of data transferred and can reduce the time needed to open the document.

Current support for ClickOnce and DirectInvoke in Microsoft Edge

Support for ClickOnce and DirectInvoke:

- ClickOnce and DirectInvoke are supported out of the box for all Windows users.

  > **NOTE**
  > Users that want to disable ClickOnce support can go to *edge://flags/#edge-click-once* and select **Disabled** from the dropdown list. You'll have to **Restart** the browser.

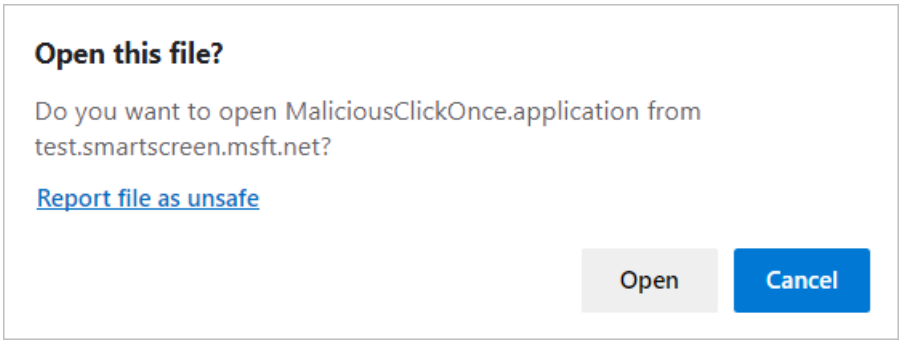
- ClickOnce and DirectInvoke aren't supported on any platforms other than Windows.

ClickOnce and DirectInvoke file handling security

ClickOnce and DirectInvoke are protected by Microsoft 365 Defender SmartScreen's URL reputation scanning service.

If a ClickOnce or a DirectInvoke request is flagged by the Microsoft 365 Defender SmartScreen URL reputation service as unsafe, users with ClickOnce or DirectInvoke enabled will see two popups.

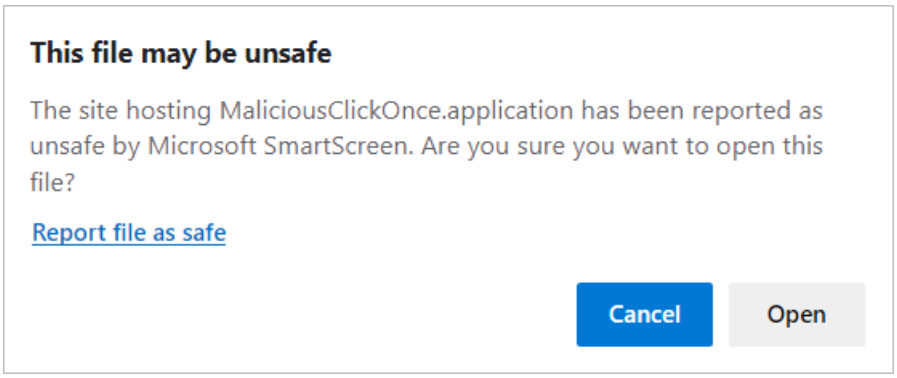
The first popup asks the user if they want to open the file. This popup is displayed regardless of whether the file was flagged as safe or unsafe. The user can **Report the file as unsafe**, **Cancel** the request, or select **Open** to continue.



If the user tries to open the file, and the file was flagged as unsafe, a second popup is displayed. This popup warns the user that the file was flagged as unsafe, and asks them if they're sure they want to download the file.

The second popup only shows up if:

- the file is a ClickOnce or DirectInvoke file
- ClickOnce or DirectInvoke are enabled
- the file is flagged as unsafe


This file may be unsafe
The site hosting MaliciousClickOnce.application has been reported as unsafe by Microsoft SmartScreen. Are you sure you want to open this file?
Report file as safe
Cancel
Open

> **NOTE**
> If ClickOnce or DirectInvoke are disabled, requested files are treated as regular downloads and if flagged as unsafe, will be marked as unsafe. This is consistent with the treatment of other unsafe downloads.

ClickOnce and DirectInvoke policies

There are two group policies that you can use to enable or disable ClickOnce and DirectInvoke for enterprise users. These two policies are ClickOnceEnabled and DirectInvokeEnabled. These two policies are labeled in the Group Policy Editor as "Allow users to open files using the ClickOnce protocol" and "Allow users to open files using the DirectInvoke protocol" respectively.

To specify file type(s) that the ClickOnce or DirectInvoke prompts should be bypassed for, use the policy labeled in the Group Policy Editor as "List of file types that should be automatically opened on download". This policy setting will let specified file types to be automatically opened after download for all domains.

You can bypass the ClickOnce or DirectInvoke prompts for specific file types for specific domains by setting up two more policies. These policies are labeled in the Group Policy Editor as "List of file types that should be automatically opened on download" and "URLs where AutoOpen-FileTypes can apply".

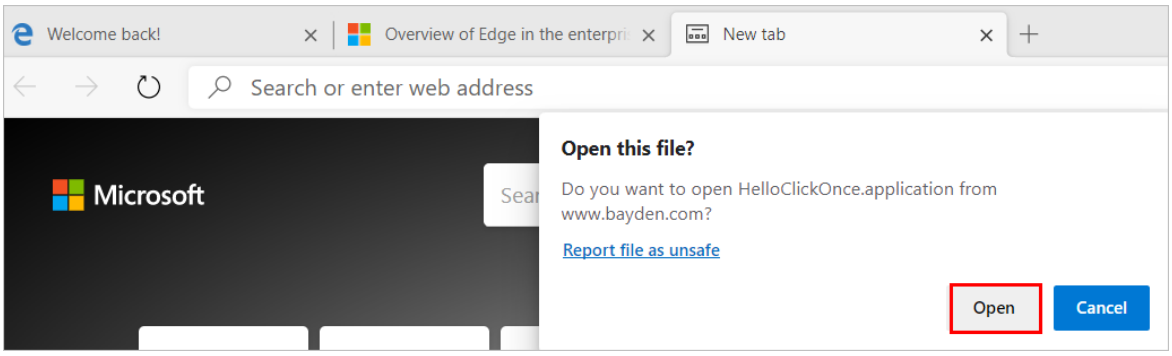
> **NOTE**
> The policy "URLs where AutoOpen- FileTypes can apply" is a supporting policy for "List of file types that should be automatically opened on download" and does nothing on its own.
>
> To get the ClickOnce protocol launch behavior, the ClickOnceEnabled policy must not be configured as Disabled, even if the AutoOpenFileTypes "List of file types that should be automatically opened on download" policy is set.

ClickOnce and DirectInvoke behavior

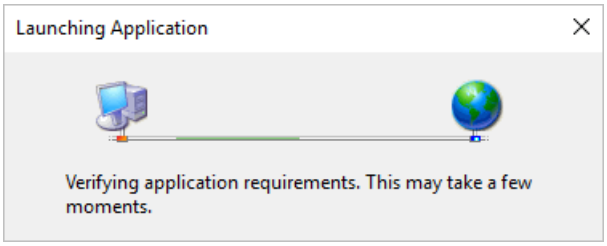
The following examples show file handling when ClickOnce and DirectInvoke are enabled or disabled.

ClickOnce enabled

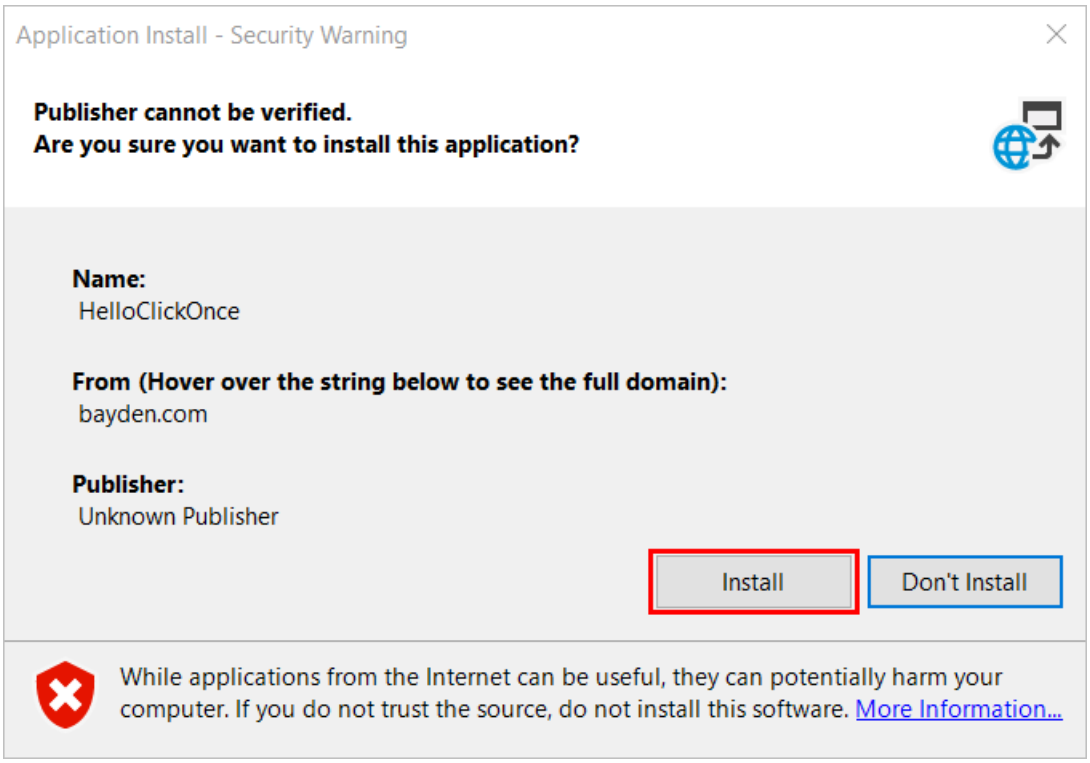
1. A user opens a link to a page that requests ClickOnce support and gets the prompt in the next screenshot.



2. After the user selects **Open**, ClickOnce attempts to launch the application.



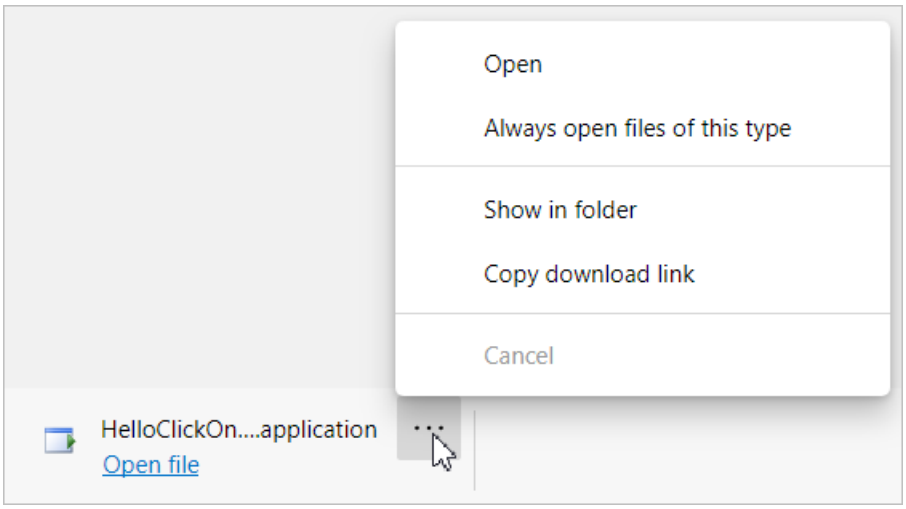
3. After the user selects **Open**, the browser shows a popup that asks the user if they're sure they want to install the application.


Application Install - Security Warning
Publisher cannot be verified.
Are you sure you want to install this application?
Name:
HelloClickOnce
From (Hover over the string below to see the full domain):
bayden.com
Publisher:
Unknown Publisher
Install
Don't Install
While applications from the Internet can be useful, they can potentially harm your computer. If you do not trust the source, do not install this software. More Information...

> **NOTE**
>
> The interface, messaging, and options shown by the ClickOnce file handler will vary depending on the type and configuration of the file that's accessed.

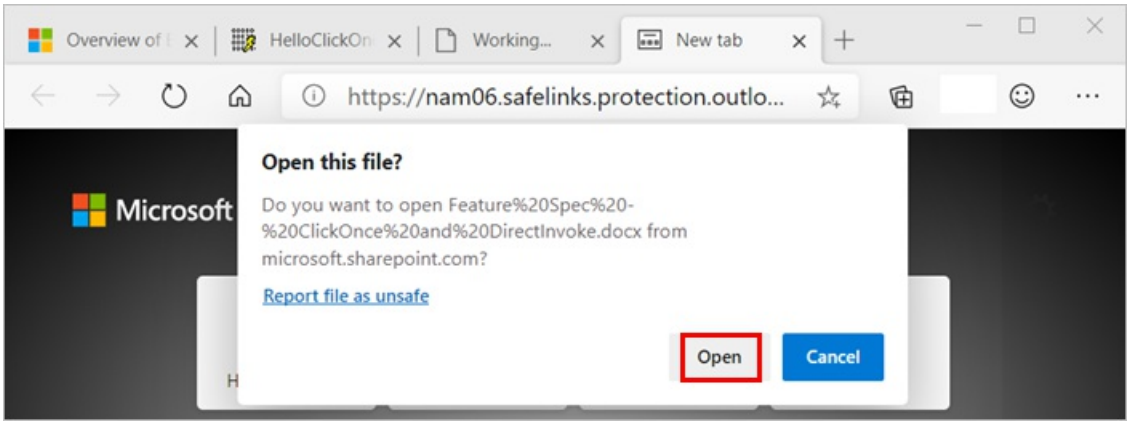
ClickOnce disabled

1. When a user opens a link to a page that requests ClickOnce support, they'll see a message in the download tray that is similar to the one in the next screenshot.



DirectInvoke enabled

1. A user opens a link to a page that requests DirectInvoke support and gets the prompt in the next screenshot.

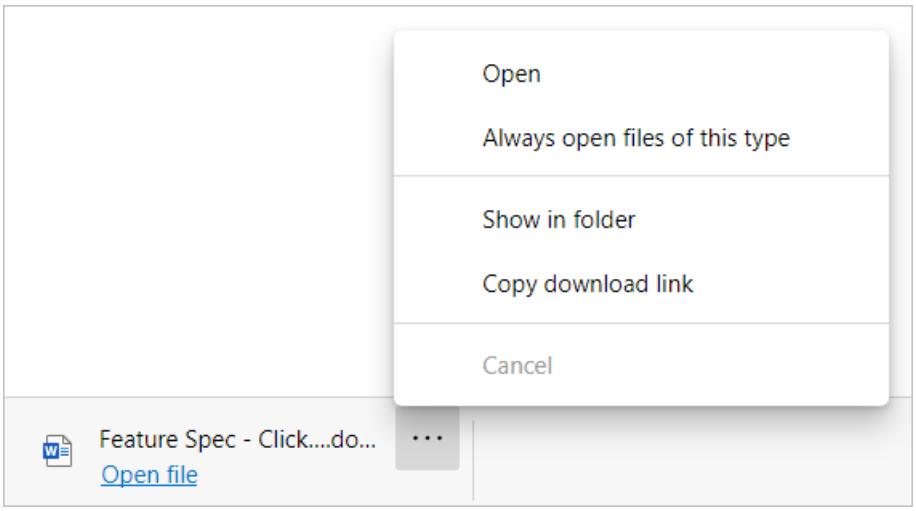


2. When the user selects **Open**, the requested file handler is opened. In this example, Microsoft Word is used to open the document that's shown in the previous screenshot.

> **NOTE**
> The interface, messaging, and options shown by the DirectInvoke file handler will vary depending on the type and configuration of the file that's accessed.

DirectInvoke disabled

1. When a user opens a link to a page that requests DirectInvoke support, DirectInvoke behaves the same as when ClickOnce is disabled. They'll see a message in the download tray that's similar to the one in the next screenshot.



See also

- ClickOnce security and deployment
- DirectInvoke in Internet Explorer
- Microsoft Edge Enterprise landing page

How to use Microsoft Edge command-line options to configure proxy settings

11/1/2022 • 2 minutes to read • Edit Online

This article describes how you can use command-line options to override the default system network settings.

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

System network settings

The Microsoft Edge network stack uses the system network settings by default. These settings include *proxy settings*, and *certificate and private key stores*.

There are scenarios where users request an alternative to using the system's default proxy settings. To support these scenarios, Microsoft Edge supports command-line options that you can use to configure custom proxy settings.

These command-line options correspond to the following policies in the **Proxy server** group:

- ProxyBypassList
- ProxyMode
- ProxyPacUrl
- ProxyServer
- ProxySettings

Command-line options for proxy settings

Microsoft Edge supports the following proxy-related command-line options.

`--no-proxy-server`

Tells Microsoft Edge not to use a Proxy, even if the system is otherwise configured to use one. It overrides any other proxy settings that are provided.

`--proxy-auto-detect`

Tells Microsoft Edge to try and automatically detect your proxy configuration. This argument is ignored if `--proxy-server` is configured.

`--proxy-server=<scheme>=<uri>[:<port>][;...] | <uri>[:<port>] | "direct://"`

Tells Microsoft Edge to use a custom proxy configuration. You can specify a custom proxy configuration in three ways.

1. Provide a semicolon-separated mapping of list scheme to url/port pairs. For example, `--proxy-server="http=proxy1:8080;ftp=ftpproxy"` tells Microsoft Edge to use HTTP proxy "proxy1:8080" for http URLs and HTTP proxy "ftpproxy:80" for ftp URLs.
2. By providing a single uri with optional port to use for all URLs. For example, `--proxy-server="proxy2:8080"` will use the proxy at "proxy2:8080" for all traffic.

3. By using the special "direct://" value. For example, `--proxy-server="direct://"` will make all connections not use a proxy.

> **NOTE**
>
> You can configure Microsoft Edge to try using a proxy and fallback to going direct if the proxy isn't available. For example, `--proxy-server="http://proxy2:8080,direct://"`.

`--proxy-bypass-list=(<trailing_domain>|<ip-address>)[:<port>][;...]`

Tells Microsoft Edge to bypass any specified proxy for the specified semicolon-separated list of hosts. This flag must be used with `--proxy-server`.

> **NOTE**
>
> Trailing-domain matching doesn't require "." separators, "*microsoft.com" will match "imicrosoft.com". For example, `--proxy-server="proxy2:8080" --proxy-bypass-list="*.microsoft.com;*example.com;127.0.0.1:8080"` will use the proxy server "proxy2" on port 8080 for all hosts except requests for *.microsoft.com, example.com, and 127.0.0.1 on port 8080. In the previous example, imicrosoft.com requests will still be proxied. However, iexample.com requests will bypass the proxy because *example.com was specified instead of *.example.com.

`--proxy-pac-url=<pac-file-url>`

Tells Microsoft Edge to use the PAC file at the specified URL. For example, `--proxy-pac-url="https://wpad/proxy.pac"` tells Microsoft Edge to resolve proxy information for URL requests using the **proxy.pac** file.

Content license

> **NOTE**
>
> Portions of this page are modifications based on work created and shared by Chromium.org and used according to terms described in the Creative Commons Attribution 4.0 International License. The original page can be found here.

This work is licensed under a Creative Commons Attribution 4.0 International License.

See also

- To see advanced configuration settings and additional options, consult the proxy documentation in the Chromium Open Source project.
- Microsoft Edge Enterprise landing page

Configurable Microsoft Edge commands

11/1/2022 • 4 minutes to read • Edit Online

This article describes the Microsoft Edge commands that can be configured via the ConfigureKeyboardShortcuts policy. To see a list of all the available shortcuts in Microsoft Edge, see Keyboard shortcuts in Microsoft Edge.

Configurable commands

The following table shows the configurable commands, how to use them, and what they do.

COMMAND	DEFAULT SHORTCUTS	DOES THIS
back	Alt + Left arrow	Go back one page
caret_browsing_toggle	F7	Turn caret browsing on or off
clear_browsing_data	Ctrl + Shift + Delete	Open clear browsing data options
close_find_or_stop	Esc	Stop loading page; Close Find dialog when it's not in focus
close_tab	Ctrl + W or Ctrl + F4	Close the current tab
close_window	Ctrl + Shift + W or Alt + F4	Close the current window
collections	Ctrl + Shift + Y	Open Collections
dev_tools	Ctrl + Shift + I	Open Developer Tools
dev_tools_console	Ctrl + Shift + J	Open Developer Tools to the Console tab
dev_tools_elements	Ctrl + Shift + C	Open Developer Tools to the Elements tab
dev_tools_toggle	F12	Open or close Developer Tools
downloads	Ctrl + J	Open Downloads
duplicate_tab	Ctrl + Shift + K	Duplicate the current tab
favorite_all_tabs	Ctrl + Shift + D	Save all open tabs as favorites in a new folder
favorite_this_tab	Ctrl + D	Save the current tab as a favorite
favorites	Ctrl + Shift + O	Open Favorites
find	Ctrl + F	Open Find on page

COMMAND	DEFAULT SHORTCUTS	DOES THIS
find_next	Ctrl + G or F3	Jump to the next match for Find on page
find_previous	Ctrl + Shift + G or Shift + F3	Jump to the previous match for Find on page
focus_address_bar	Alt + D or Ctrl + L or F4	Select the URL in the address bar to edit
focus_app_toolbar	Alt + Shift + T	Set focus to the first item in the app bar toolbar
focus_favorites	Alt + Shift + B	Set focus to the first item in the favorites bar toolbar
focus_inactive_notification	Alt + Shift + A	Set focus to infobar or notification
focus_next_pane	F6	Set focus to the next pane or notification
focus_previous_pane	Shift + F6	Set focus to the previous pane or notification
focus_reading_bar	Alt + Shift + R	Set focus to the first item in the Immersive Reader toolbar
focus_search	Ctrl + E or Ctrl + K	Open a search query in the address bar
focus_settings_and_more	Alt or F10	Set focus to the Settings and more "..." button
focus_web_pane	Ctrl + F6	Set focus to the web page
forward	Alt + Right arrow	Go forward one page
fullscreen	F11	Enter or exit full screen
help_page	F1	Open Microsoft Edge support page
history	Ctrl + H	Open History
home	Alt + Home	Open your home page in the current tab
immersive_reader_toggle	F9	Enter or exit Immersive Reader
mute_tab_toggle	Ctrl + M	Mute or unmute the current tab
new_application_guard_window	Ctrl + Shift + Q	Open a new Application Guard window

COMMAND	DEFAULT SHORTCUTS	DOES THIS
new_inprivate_window	Ctrl + Shift + N	Open a new InPrivate window
new_tab	Ctrl + T	Open a new tab and switch to it
new_window	Ctrl + N	Open a new window
open_file	Ctrl + O	Open a file from your computer in Microsoft Edge
paste_and_go	Ctrl + Shift + L	Paste and search or Paste and go (if it's a URL)
print	Ctrl + P	Print the current page in Microsoft Edge
profile	Ctrl + Shift + M	Sign in as a different user or browse as a Guest
read_aloud_toggle	Ctrl + Shift + U	Start or stop Read Aloud
refresh	Ctrl + R or F5	Refresh the current page
refresh_bypassing_cache	Ctrl + Shift + R or Shift + F5	Refresh the current page, ignoring cached content
reopen_tab	Ctrl + Shift + T	Reopen the last closed tab, and switch to it
save_page	Ctrl + S	Save the current page
select_last_tab	Ctrl + 9	Switch to the last tab
select_next_tab	Ctrl + Tab or Ctrl + PgDn	Switch to the next tab
select_previous_tab	Ctrl + Shift + Tab or Ctrl + PgUp	Switch to the previous tab
select_tab_0 [1, 2, ... 7]	Ctrl + 1, 2, ... 8	Switch to a specific tab
send_feedback	Alt + Shift + I	Open the Send feedback dialog
settings_and_more_menu	Alt + E or Alt + F	Open the Settings and more "..." menu
show_favorites_bar_toggle	Ctrl + Shift + B	Show or hide the favorites bar
sidebar_search_selected_text	Ctrl + Shift + E	Search for the currently selected text in the sidebar
system_print	Ctrl + Shift + P	Print the current page using the system dialog
task_manager	Shift + Esc	Open Browser task manager

COMMAND	DEFAULT SHORTCUTS	DOES THIS
vertical_tabs_toggle	Ctrl + Shift + ,	Turn Vertical tabs on or off
view_source	Ctrl + U	View source
web_capture	Ctrl + Shift + S	Start Web capture
web_select	Ctrl + Shift + X	Start Web select
zoom_in	Ctrl + Plus (+)	Zoom in
zoom_out	Ctrl + Minus (-)	Zoom out
zoom_reset	Ctrl + 0 (zero)	Reset page zoom level

See also

- Microsoft Edge Enterprise landing page

Filter format for URL list-based policies

11/1/2022 • 3 minutes to read • Edit Online

This article describes the filter format used for the Microsoft Edge URL list-based policies (For example, URLBlocklist, URLAllowList, and CertificateTransparencyEnforcementDisabledForUrls policies.

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

The filter format

The filter format is:

```
[scheme://][.]host[:port][/path][@query]
```

The fields in the filter format are:

FIELD	DESCRIPTION
scheme (*optional*)	It can be http://, https://, ftp://, edge://, etc.
host (*required*)	It must be a valid host name and you can use a wildcard ("*"). To disable subdomain matching, include an optional dot (".") before **host**. A single IP Address Literal hostname may be specified, but wildcarding is not supported for an IP Address Literal hostname.
port (*optional*)	Valid values range from 1 to 65535.
path (*optional*)	You can use any string in the path.
query (*optional*)	The **query** is either key-value or key-only tokens separated by an ampersand ("&"). Separate key-value tokens with an equal sign ("="). To indicate a prefix match, you can use an asterisk ("*") at the end of the **query**.

Comparing the filter format to the URL format

The filter format resembles the URL format, except for the following differences:

- If you include "user:pass", it will be ignored. For example, http://user:pass@ftp.contoso.com/pub/example.iso.
- If you include a fragment identifier ("#"), it and everything that follows the identifier is ignored.
- You can use a wildcard ("*") as the **host** and you can prefix it with a dot (".").
- You can use a forward slash ("/") or a dot (".") as a suffix for the **host**. In this case, the suffix is ignored.

Filter selection criteria

The filter selected for a URL is the most specific match found after processing the following filter selection rules:

1. Filters with the longest **host** match are selected first.
2. From the selected filters, any filter with a non-matching scheme or port is discarded.
3. From the remaining filters, the filter with the longest matching **path** is selected.
4. From the remaining filters, the filter with the longest set of query tokens is selected. At this step, the allow list filter takes precedence over the block list filter if both filters have the same **path** length and number of **query** tokens.
5. If there's no valid filter remaining, then the left-most subdomain is removed from **host** and the selection process starts over at step 1. The special asterisk ("*") **host** is the last searched and it matches all hosts.
6. If a filter's available, it blocks or allows the URL request.

> **NOTE**
> The default behavior is to allow the URL request if no filter is matched.

Example filter selection criteria

In this example, when searching for a match to "https://sub.contoso.com/docs" the filter selection will:

1. Search for a filter for "sub.contoso.com". If it finds a filter, the search moves to step 2. If a filter isn't found, then it tries again with "contoso.com", "com", and finally "".
2. From the selected filters, any that don't have "http" in the **scheme** are removed.
3. From the remaining filters, any that have an exact port number that isn't "80" are removed.
4. From the remaining filters, any that don't have "/docs" as a prefix of the **path** are removed.
5. From the remaining filters, the filter with the longest path prefix is selected and applied. If a filter isn't found, the selection process starts over again at step 1. The process is repeated with the next subdomain.

Additional filter information

If a filter has a dot (".") prefixing the **host** then only exact **host** matches are filtered. For example:

- "contoso.com" (no dot) will match "contoso.com", "www.contoso.com", and "sub.www.contoso.com"
- ".www.contoso.com" (with a dot prefix) will only match "www.contoso.com"

You can use either a standard or custom **schema**. Supported standard schemas include:

- *about*, *blob*, *content*, *edge*, *cid*, *data*, *file*, *filesystem*, *ftp*, *gopher*, *http*, *https*, *javascript*, *mailto*, *ws*, and *wss*.

Any other **schema** is treated as a custom **schema**, but only the *schema:** and *schema://** patterns are allowed. For example:

- "custom:*" or "custom://*" will match "custom:app"
- "custom:app" or "custom://app" are invalid

schema and **host** aren't case-sensitive. For example:

- "http://contoso.com" filter matches "HTTP://contoso.com", "http://contoso.COM", and "http://contoso.com"

path and **query** are case-sensitive. For example:

- "http://contoso.com/path?query=A" filter doesn't match "http://contoso.com/Path?query=A" or "http://contoso.com/path?Query=A". It does match "http://contoso.COM/path?query=A".

Content license

NOTE

Portions of this page are modifications based on work created and shared by Chromium.org and used according to terms described in the Creative Commons Attribution 4.0 International License. The original Chromium page can be found here.

This work is licensed under a Creative Commons Attribution 4.0 International License.

See also

- Microsoft Edge Enterprise landing page

Microsoft Edge will disable modifying `document.domain`

11/1/2022 • 4 minutes to read • Edit Online

NOTE

This article applies to Microsoft Edge Stable version 109 or later.

WARNING

If your website relies on relaxing the same-origin policy via `document.domain`, your action is required. Continue to read more about why this is changing or go to the Alternative cross-origin communication to learn about alternative mechanisms to achieve cross-origin communication.

Introduction

The "domain" property of the Document interface gets or sets the domain part of the origin of the current document, as used by the same-origin policy.

Starting in Microsoft Edge version 109, attempts to modify the `document.domain` property using JavaScript will be ignored. You'll need to use alternative approaches, such as `postMessage()` or the Channel Messaging API, to communicate cross-origin.

As an alternative, if your website relies on same-origin policy relaxation via `document.domain` to function correctly, the site may send an `Origin-Agent-Cluster: ?0` header; this header must be sent from all other documents that require the relaxation.

NOTE

`document.domain` has no effect if only one document sets it.

Why make `document.domain` immutable?

Some websites set `document.domain` to allow communication between "same-site but cross-origin" pages. Setting `document.domain` makes it possible for same-site documents to communicate more easily. Because this change relaxes the same-origin policy, a parent page can access a same-site iframe's document and traverse the DOM tree, and vice versa.

IMPORTANT

Same-site but cross-origin sites have the same eTLD+1 but different subdomains.

Let's say a page on `https://parent.example.com` embeds an iframe page from `https://video.example.com`. These pages have the same eTLD+1 (`example.com`) with different subdomains. When both pages' `document.domain` is set to `'example.com'`, the browser treats the two pages as if they're same-origin.

This technique is convenient; but it introduces a security risk.

Security concerns with `document.domain`

Security concerns around `document.domain` have led to a change in the specification that warns developers about this concern and tells them to avoid using it if possible. The current discussion with other browser vendors is moving in the same direction.

The following examples show how an attacker can abuse `document.domain`.

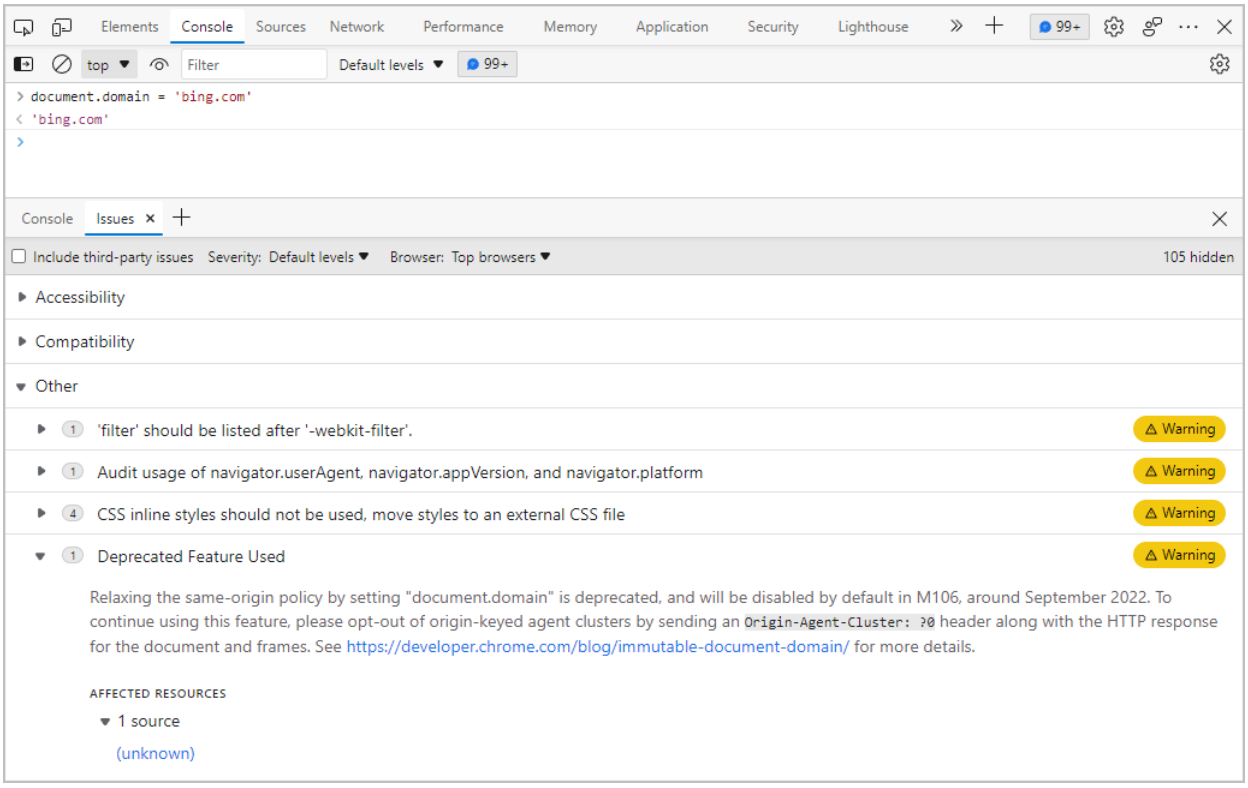
Consider a shared hosting service that provides a unique subdomain to each customer. If a developer sets `document.domain` in their page, an attacker's page served from a different subdomain can set the same value and modify the content of the victim page.

Similarly, consider a shared hosting service that serves pages using a different port for each customer. If a developer sets `document.domain` in their page, an attacker's page served from a different port can set the same value and modify the content of the victim page. This attack is possible because `document.domain` ignores the port number component of the origin.

> **NOTE**
>
> To learn more about the security implications of setting `document.domain`, read the Document.domain article on MDN.

How will I know if my site is affected?

If your website is affected by this change, Microsoft Edge will show a warning in the DevTools Issues panel. The following screenshot shows an example of this warning.



If you have a reporting endpoint set up, you'll also be sent deprecation reports. Learn more about how to use the Reporting API with existing report collection services or by building your own reporting solution.

TIP

You can run your site through the LightHouse deprecated API audit to find all APIs that are scheduled to be removed from Microsoft Edge.

Alternative cross-origin communication

Currently you have two options to replace `document.domain` for your website. In most use cases, cross-origin postMessage() or the Channel Messaging API can replace `document.domain`.

The following list shows the steps a developer needs to take to use `postMessage()` instead of `document.domain` for cross-origin DOM manipulation.

1. `https://parent.example.com` sends a message via `postMessage()` to an iframe containing `https://video.example.com` asking it to modify its own DOM.
2. `https://video.example.com` manipulates its DOM and uses `postMessage` to notify the parent of its success.
3. `https://parent.example.com` acknowledges the success.

For step 1 on `https://parent.example.com`:

```
// Configure a handler to receive messages from the subframe.
iframe.addEventListener('message', (event) => {

// Reject all messages except from https://video.example.com
  if (event.origin !== 'https://video.example.com') return;

  // Filter success messages
    if (event.data === 'succeeded') {

    // DOM manipulation is succeeded

  }

});

// Send a message to the subframe at https://video.example.com

iframe.postMessage('Request DOM manipulation', 'https://video.example.com');
```

For step 2 on `https://video.example.com`:

```
// Configure a handler to receive messages from the parent frame.
window.addEventListener('message', (event) => {

  // Reject all messages except ones from https://parent.example.com

  if (event.origin !== 'https://parent.example.com') return;

  // Perform requested DOM manipulation on https://video.example.com.

  if (event.data === "showTheButton") {
     document.getElementById('btnContinue').style.visibility = 'visible';
     // Send a success message back to the parent.

     event.source.postMessage('succeeded', event.origin);
  }
});
```

Send the `Origin-Agent-Cluster: ?0` header as a last resort

If you have strong reasons to continue setting `document.domain`, you can send `Origin-Agent-Cluster: ?0` response header on the target document.

```
Origin-Agent-Cluster: ?0
```

The `Origin-Agent-Cluster` header instructs the browser whether the document should be handled by the origin-keyed agent cluster or not. To learn more about `Origin-Agent-Cluster`, read Requesting performance isolation with the Origin-Agent-Cluster header.

When you send this header, your document can continue to set `document.domain` even after it becomes immutable by default.

Browser compatibility

The following organizations support deprecating `document.domain` in the interest of browser compatibility.

- The Origin specification, states that the feature should be removed.
- The Mozilla standards position considers disabling `document.domain` by default worth prototyping.
- WebKit indicates that they're moderately positive about deprecating `document.domain` setter.

Other resources

- Document.domain
- Origin Isolation and Deprecating `document.domain`
- Deprecating `document.domain` setter

Content license

NOTE

Portions of this page are modifications based on work created and shared by Chromium.org and used according to terms described in the Creative Commons Attribution 4.0 International License. The original page can be found here.

This work is licensed under a Creative Commons Attribution 4.0 International License.

Learn how Microsoft Edge handles mixed content downloads

11/1/2022 • 2 minutes to read • Edit Online

This article defines mixed content downloads and explains how Microsoft Edge handles them.

> **NOTE**
> This article applies to Microsoft Edge version 85 or later.

What are mixed content downloads?

A mixed content download happens when you start a download from an HTML page that was loaded over a secure HTTPS connection, but one of the following conditions exists:

- One or more of the download location's redirects was loaded over an insecure HTTP connection.
- The final download location was loaded over an insecure HTTP connection.

Either of the preceding scenarios is a mixed content download because the request was made using secure HTTPS and both HTTP and HTTPS connections are used to reach the final destination. Modern browsers display warnings about this type of content to indicate that this download may be transferred insecurely even though the original page was accessed securely.

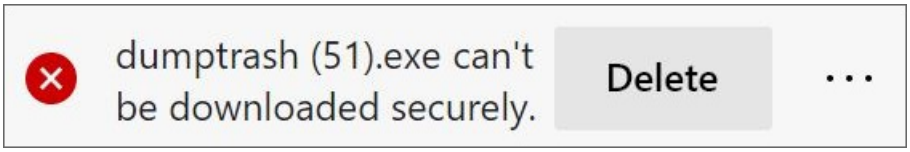
Download warnings and user options

The download warning ensures that users know that the file they're downloading could be read by malicious attackers on their network. This warning lets a user make an informed decision on whether to download the file.

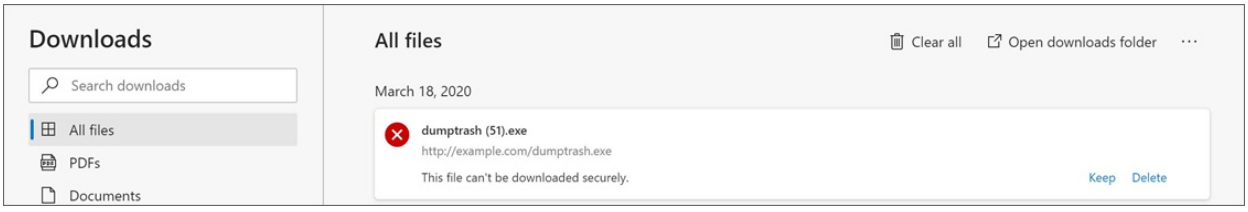
In Microsoft Edge, mixed content downloads will be blocked but users can override and download the file if they want to. Microsoft Edge plans on starting to block mixed content executable file downloads starting with Microsoft Edge version 85 and will block different filetypes in future releases.

> **NOTE**
> Deployment of this feature is subject to change based on release schedule and user feedback.

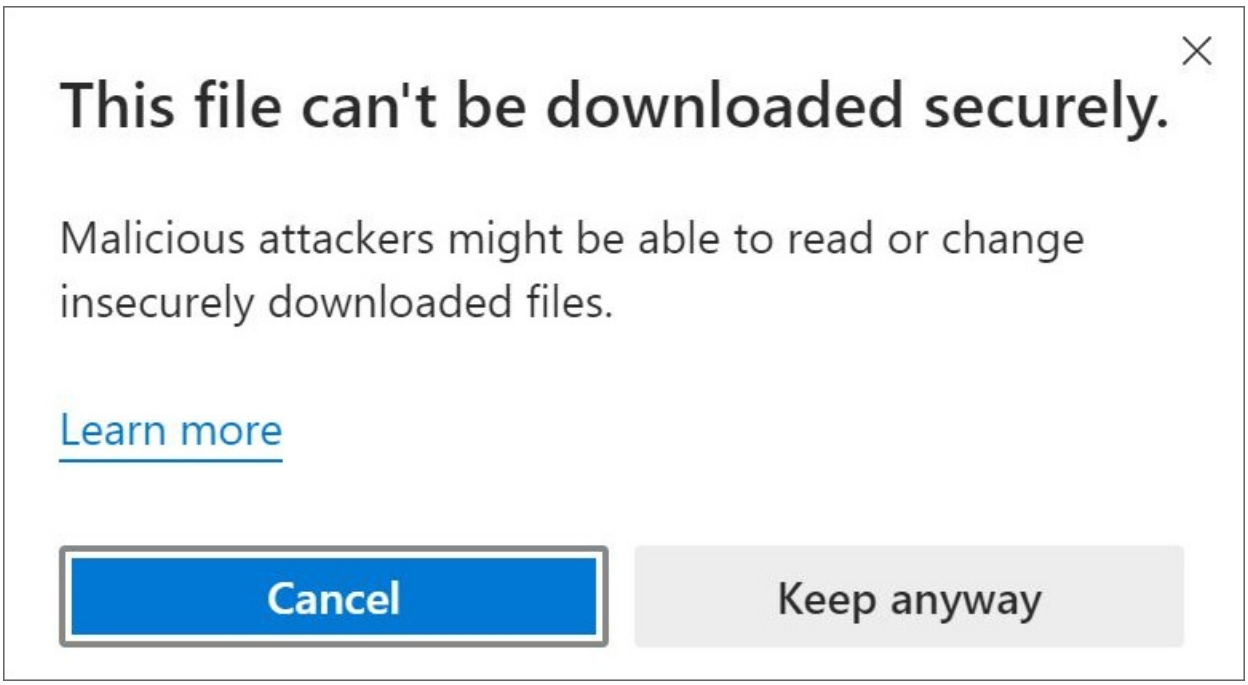
In the download shelf, the block warning message looks like the example in the next screenshot.



On the download page, the block warning looks like the following screenshot example:



If a user decides to keep the download, they are prompted to confirm their action. The next screenshot shows an example of this confirmation prompt.


This file can't be downloaded securely.
Malicious attackers might be able to read or change insecurely downloaded files.
Learn more
Cancel
Keep anyway

Supporting policies

Enterprises that want to exclude mixed content blocking from specific websites can use the InsecureContentAllowedForUrls policy to do so.

Content license

NOTE

Portions of this page are modifications based on work created and shared by Chromium.org and used according to terms described in the Creative Commons Attribution 4.0 International License. The original page can be found here.

This work is licensed under a Creative Commons Attribution 4.0 International License.

See also

- Microsoft Edge Enterprise landing page

Progressive rollouts for Microsoft Edge Stable channel updates

11/1/2022 • 2 minutes to read • Edit Online

Starting with Microsoft Edge 83 release, we will perform gradual rollouts of major updates to Microsoft Edge Stable channel over the span of a few days. This progressive rollout allows us to monitor upgrades and safely update the browser across the organization.

> **NOTE**
> This applies to Microsoft Edge Stable channel version 83 or later.

Why do we need progressive rollout?

By monitoring the health of our updates closely and rolling out the updates over the course of several days, we can limit the impact of issues that might occur with the new update. With Microsoft Edge release 83, Progressive Rollouts will be enabled for all Windows 7, Windows 8 & 8.1, and Windows 10 versions of Microsoft Edge. We will support Microsoft Edge on Mac as soon as it is ready.

How will the updates work?

Each installation of Microsoft Edge is assigned an upgrade value. When we start rolling out incrementally, you'll see the update when the value on your device falls within the upgrade value range. As the rollout progresses (within a few days), all users will eventually get the update. Browser updates with critical security fixes will have a faster rollout cadence than updates that don't have critical security fixes. This is done to ensure prompt protection from vulnerabilities.

How does this affect enterprises?

Microsoft Edge artifacts are distributed to enterprises using multiple mechanisms such as Microsoft Intune, Windows Server Update Service (WSUS), and Configuration Manager. These deployment tools behave differently with respect to Progressive Rollout:

- Enterprises that manage distribution via Microsoft Intune are registered for auto-updates. Progressive Rollout is used, and all the users will see an update in a few days.
- Enterprises that manage distribution through WSUS (Windows Server Update Services) or Configuration Manager are not registered for auto-updates. Administrators manage and apply the updates that will be available from the start. Progressive Rollout does not affect this process.

Please share your valuable feedback through user voice, the in-application feedback button, or below in the comments if you have any concerns or questions.

See also

- Microsoft Edge Enterprise landing page

Provision favorites for Microsoft Edge

11/1/2022 • 2 minutes to read • Edit Online

Based on customer feedback, we've made improvements to provisioning favorites. Starting with Microsoft Edge version 85, Admins no longer have to manually craft a file to provision favorites. Admins can add favorites and folders using the Microsoft Edge UI to generate a file that can be exported to a group policy.

This article describes how to provision a set of favorites and folders for your organization. You can use the Configure favorites policy to provision favorites and folders.

> **NOTE**
> This article applies to Microsoft Edge version 85 or later.

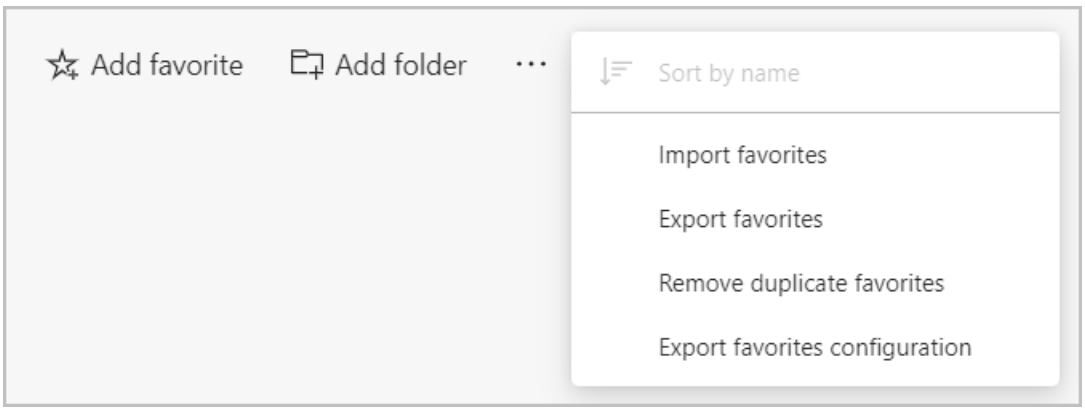
Prerequisites and recommendations

- Microsoft Edge version 85 with the appropriate administrative template installed for group policies.
- We recommend that you use a new profile in Microsoft Edge to provision these favorites. All favorites that are saved with the profile will be included in the export.

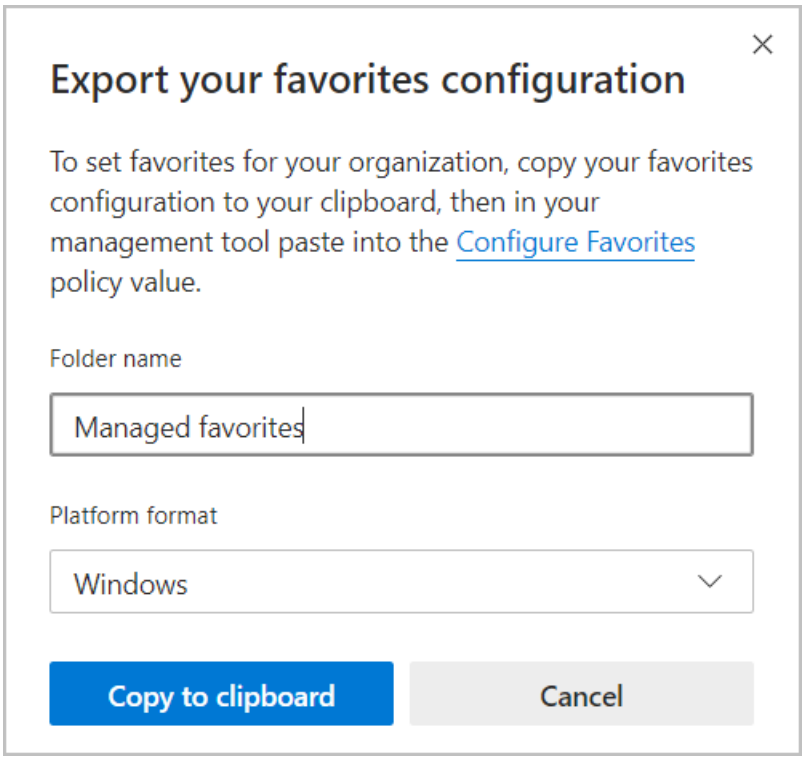
Provision favorites and folders

Use the following steps to provision favorites and folders for your users.

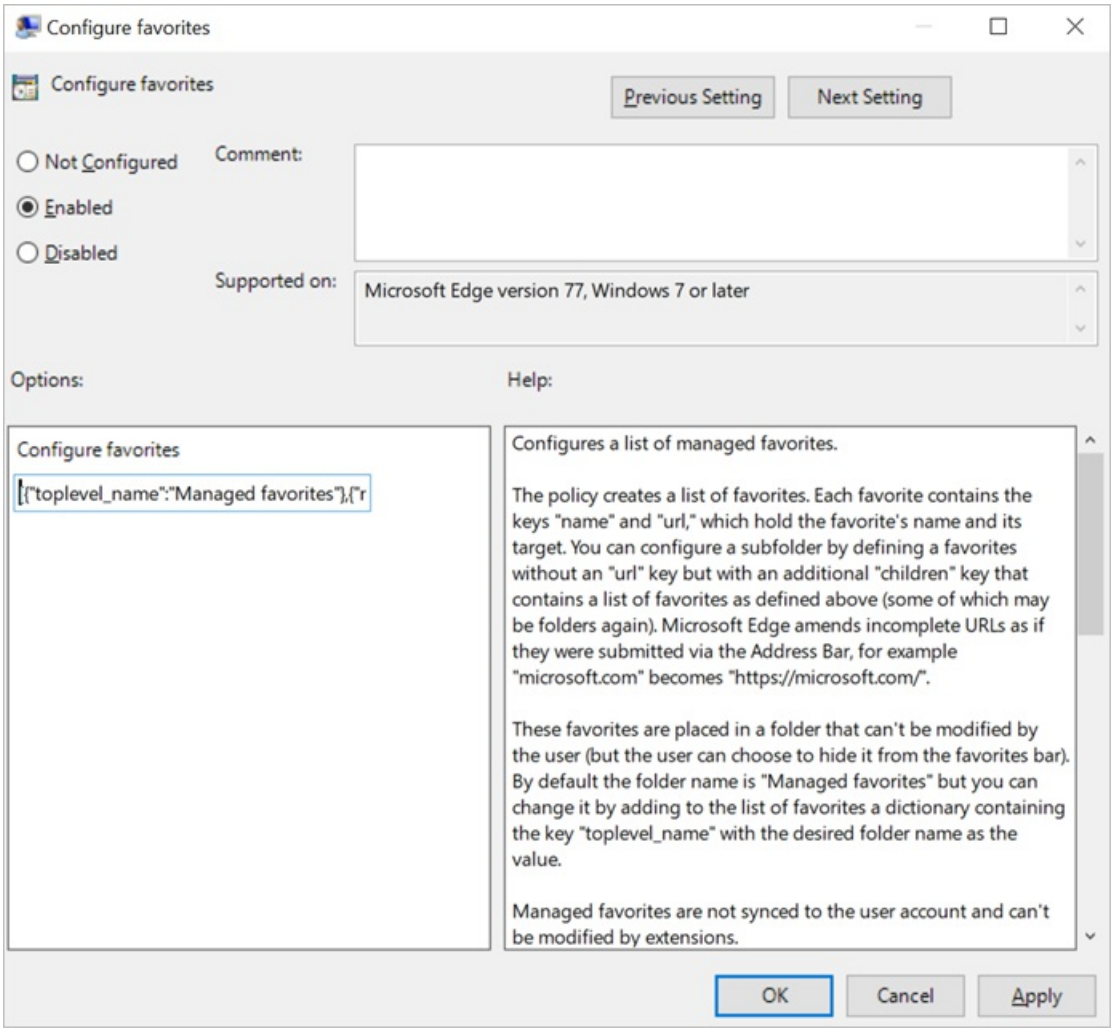
1. Go to the Microsoft Edge address bar and type this URL: *edge://flags/#edge-favorites-admin-export*.
2. Under **Favorites configuration export for administrators**, pick **Enabled** from the dropdown list and then select **Restart**.
3. Go to the **Favorites** page at *edge://favorites* so you can add the favorites and folders that you want to provision.
4. When you finish adding favorites and folders you'll export them so they can be used by the **Configure favorites** policy. Go to the address bar and navigate to *edge://favorites*, select the ellipsis "..." and choose **Export favorites configuration**. The next screenshot shows the options you have when provisioning favorites.



5. Under **Export your favorites configuration** you provide a name for the folder that your users will see. Type the Folder name and pick the Platform format you want to use. Select **Copy to clipboard**. The next screenshot shows "Managed favorites" for the folder name and the platform is Windows.


Export your favorites configuration
To set favorites for your organization, copy your favorites configuration to your clipboard, then in your management tool paste into the Configure Favorites policy value.
Folder name
Managed favorites
Platform format
Windows
Copy to clipboard
Cancel

6. Open the Group Policy Editor, navigate to *Computer Configuration/Administrative Templates/* and pick **Configure Favorites**. Enable the "Configure Favorites" policy. Under **Options:**, paste the exported contents in the Configure favorites text area then select **Apply**. The next screenshot shows an example of the "Managed favorites" folder from step 5.


Configure favorites
Configure favorites
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
Microsoft Edge version 77, Windows 7 or later
Options:
Help:
Configure favorites
[{"toplevel_name":"Managed favorites"},{"r
Configures a list of managed favorites.
The policy creates a list of favorites. Each favorite contains the keys "name" and "url," which hold the favorite's name and its target. You can configure a subfolder by defining a favorites without an "url" key but with an additional "children" key that contains a list of favorites as defined above (some of which may be folders again). Microsoft Edge amends incomplete URLs as if they were submitted via the Address Bar, for example "microsoft.com" becomes "https://microsoft.com/".
These favorites are placed in a folder that can't be modified by the user (but the user can choose to hide it from the favorites bar). By default the folder name is "Managed favorites" but you can change it by adding to the list of favorites a dictionary containing the key "toplevel_name" with the desired folder name as the value.
Managed favorites are not synced to the user account and can't be modified by extensions.
OK
Cancel
Apply

7. Select **OK** or **Apply** to save the policy settings.

See also

- Microsoft Edge Enterprise landing page

Redirection from Internet Explorer to Microsoft Edge for compatibility with modern web sites

11/1/2022 • 4 minutes to read • Edit Online

> **NOTE**
> This article applies to Microsoft Edge Stable version 87 or later.

Overview

> **NOTE**
> The retired, out-of-support Internet Explorer 11 (IE11) desktop application will be permanently disabled on certain versions of Windows 10 as part of the February 2023 Windows security update ("B") release scheduled for February 14, 2023. Learn more
>
> We highly recommend setting up IE mode in Microsoft Edge and disabling IE11 prior to this date to ensure your organization does not experience business disruption. Learn how

Many modern websites have designs that are incompatible with Internet Explorer. Whenever an Internet Explorer user visits an incompatible public site, they get a message that tells them the site is incompatible with their browser, and they need to manually switch to a different browser.

The need to manually switch to a different browser changes starting with Microsoft Edge Stable version 87.

When a user goes to a site that is incompatible with Internet Explorer, they will be automatically redirected to Microsoft Edge. This article describes the user experience for redirection and the group policies that are used to configure or disable automatic redirection.

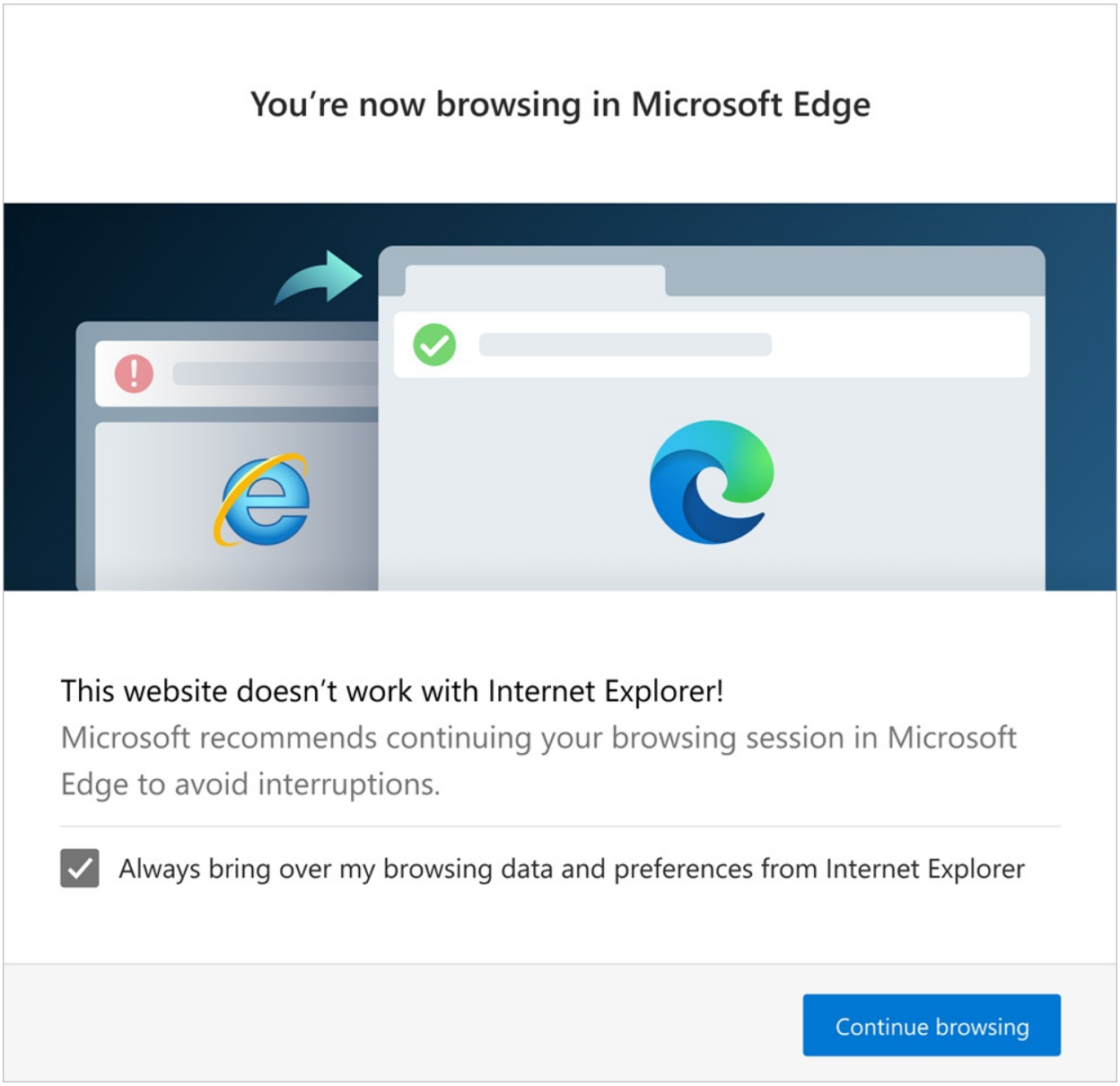
> **NOTE**
> Microsoft maintains a list of all sites that are known to be incompatible with Internet Explorer. For more information, see Request updates to the incompatible sites list

Prerequisites

- Microsoft Edge Stable version 87 or later
- Windows versions
  - Windows 10 version 1709 or later
  - Windows 8.1
  - Windows 7

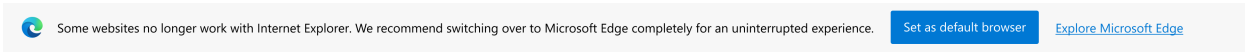
Redirection experience

On redirection to Microsoft Edge, users are shown the one-time dialog in the next screenshot. This dialog explains why they're getting redirected and prompts for consent to copy their browsing data and preferences from Internet Explorer to Microsoft Edge. The following browsing data will be imported: Favorites, Passwords, Search engines, open tabs, History, settings, cookies, and the Home Page.


You're now browsing in Microsoft Edge
This website doesn't work with Internet Explorer!
Microsoft recommends continuing your browsing session in Microsoft Edge to avoid interruptions.
Always bring over my browsing data and preferences from Internet Explorer
Continue browsing

Even if they don't give their consent by checking "Always bring over my browsing data and preferences from Internet Explorer", they can click**Continue browsing**to continue their session.

Finally, a website incompatibility banner, shown in the next screenshot, appears below the address bar for every redirection.


Some websites no longer work with Internet Explorer. We recommend switching over to Microsoft Edge completely for an uninterrupted experience.
Set as default browser
Explore Microsoft Edge

The website incompatibility banner:

- encourages the user to switch to Microsoft Edge
- offers to make Microsoft Edge as the default browser
- gives the user the option to explore Microsoft Edge

WhenasiteisredirectedfromInternetExplorertoMicrosoftEdge, theInternetExplorertabthatstarted loadingthe siteis navigated to a Microsoftsupportpagethat explains whythesitewasredirectedtoMicrosoftEdge.

> **NOTE**
> After a redirection users can go back to using Internet Explorer for sites that are not on the Internet Explorer incompatibility list.

Policies to configure redirection to Microsoft Edge

> **NOTE**
>
> These policies will be available as ADMX file updates by October 26, 2020 and will be available in Intune by November 9, 2020.

Three group policies must be configured to enable automatic redirection to Microsoft Edge. These policies are:

- RedirectSitesFromInternetExplorerPreventBHOInstall
- RedirectSitesFromInternetExplorerRedirectMode
- HideInternetExplorerRedirectUXForIncompatibleSitesEnabled

Policy: RedirectSitesFromInternetExplorerPreventBHOInstall

Redirection from Internet Explorer to Microsoft Edge requires an Internet Explorer Browser Helper Object (BHO) named "IEtoEdge BHO". The **RedirectSitesFromInternetExplorerPreventBHOInstall** policy controls whether or not this BHO is installed.

- Ifyouenablethispolicy,theBHOrequired for redirection willnotbeinstalled and your users will continue to see incompatibility messages for certain websites on Internet Explorer. If the BHO is alreadyinstalled,itwillbeuninstalledthe next time the Microsoft Edge Stable channelis updated.
- If you disable or don't configure this policy,theBHOwillbeinstalled. This is the default behavior.

In addition to needing the BHO, there is a dependency on the **RedirectSitesFromInternetExplorerRedirectMode**, which needs to be set to "Redirect sites based on the incompatible sites sitelist" or "Not Configured".

Policy: RedirectSitesFromInternetExplorerRedirectMode

This policy corresponds to the Microsoft Edge **Default browser** setting "Let Internet Explorer open sites in Microsoft Edge". You can access this setting by going to the *edge://settings/defaultbrowser* URL.

- If you don't configure this policy or set it to "Sitelist", Internet Explorer will redirect incompatible sites to Microsoft Edge. This is the default behavior.
- To disable this policy, select **Enabled** AND then in the dropdown under Options: Redirect incompatible sites from Internet Explorer to Microsoft Edge, select **Disable**. In this state, incompatible sites aren't redirected to Microsoft Edge.

> **NOTE**
>
> If you're on a personal device that isn't managed by your organization, you'll see another setting named "Allow sites to be loaded in Internet Explorer mode" under **Internet Explorer compatibility**.
>
> If you're on a domain joined or Mobile Device Management (MDM) enrolled device, you won't see this option.
>
> Instead, if you want to let your users load sites in Internet Explorer mode, you can do so by configuring the policy Allow Internet Explorer mode testing.

Policy: HideInternetExplorerRedirectUXForIncompatibleSitesEnabled

This policy configures the user experience for incompatible site redirection to Microsoft Edge.

- If you enable this policy, users never see the one-time redirection dialog and the redirection banner. No browser data or user preferences are imported.
- If you disable or don't configure this policy, theredirectiondialogwill beshownonthefirstredirectionandthepersistentredirectionbannerwillbeshownfor

sessionsthatstartwitharedirection.

> **NOTE**
> User browsingdatawillbeimportedeverytimea userencountersa new redirection. However, this only happens if the user consented to the import on the one-time redirection dialog.

Disable redirection to Microsoft Edge

If you want to disable redirection BEFORE updating to Microsoft Edge Stable version 87, use the following step:

1. Set the **RedirectSitesFromInternetExplorerPreventBHOInstall** policy to **Enabled**.

If you want to disable redirection AFTER updating to Microsoft Edge Stable version 87, use the following steps:

1. Set the **RedirectSitesFromInternetExplorerRedirectMode** policy to **Enabled** AND then in the dropdown under Options: Redirect incompatible sites from Internet Explorer to Microsoft Edge, select **Disable**. This setting will stop redirecting as soon as the policy takes effect.
2. Set the **RedirectSitesFromInternetExplorerPreventBHOInstall** policy to **Enabled**. This will uninstall the BHO after the next Microsoft Edge update.

See also

- Request updates to the incompatible sites list
- Microsoft Edge Enterprise landing page
- Microsoft Edge Policies

Regular Expression 2 (re2.h) syntax

11/1/2022 • 10 minutes to read • Edit Online

Regular expressions are a notation for describing sets of character strings. When a string is in the set described by a regular expression, we say that the regular expression *matches* the string.

The simplest regular expression is a single literal character. Except for the metacharacters like `*+?()|`, characters match themselves. To match a metacharacter, escape it with a backslash. For example, `\+` matches the literal plus character.

Two regular expressions can be altered or concatenated to form a new regular expression: if e_1 matches s and e_2 matches t, then $e_1 | e_2$ matches s or t, and $e_1\ e_2$ matches st.

The metacharacters `*`, `+`, and `?` are repetition operators: e_1 `*` matches a sequence of zero or more (possibly different) strings, each of which match e_1; e_1 `+` matches one or more; e_1 `?` matches zero or one.

Operator precedence, from weakest to strongest binding, is as follows:

- alternation
- concatenation
- repetition operators

Explicit parentheses can be used to force different meanings, as in arithmetic expressions. Some examples: `ab|cd` is equivalent to `(ab)|(cd)` ; `ab\` is equivalent to `a(b\)`.

The syntax described so far is most of the traditional Unix *egrep* regular expression syntax. This subset suffices to describe all regular languages. A regular language is a set of strings that can be matched in a single pass through the text using only a fixed amount of memory. Newer regular expression facilities (notably Perl and those languages that have copied it) have added many new operators and escape sequences. These changes make the regular expressions more concise, and sometimes more cryptic, but not more powerful.

This page lists the regular expression syntax accepted by RE2.

It also lists some syntax accepted by PCRE, PERL, and VIM.

Syntax tables

KINDS OF SINGLE-CHARACTER EXPRESSIONS	EXAMPLES
any character, possibly including newline (s=true)	.
character class	[xyz]
negated character class	[^xyz]
Perl character class (link)	\d
negated Perl character class	\D
ASCII character class (link)	[[:alpha:]]

KINDS OF SINGLE-CHARACTER EXPRESSIONS	EXAMPLES
negated ASCII character class	[[:^alpha:]]
Unicode character class (one-letter name)	\pN
Unicode character class	\p{Greek}
negated Unicode character class (one-letter name)	\PN
negated Unicode character class	\P{Greek}

	COMPOSITES
xy	x followed by y
x|y	x or y (prefer x)

	REPETITIONS
x*	zero or more x, prefer more
x+	one or more x, prefer more
x?	zero or one x, prefer one
x{n,m}	n or n+1 or ... or m x, prefer more
x{n,}	n or more x, prefer more
x{n}	exactly n x
x*?	zero or more x, prefer fewer
x+?	one or more x, prefer fewer
x??	zero or one x, prefer zero
x{n,m}?	n or n+1 or ... or m x, prefer fewer
x{n,}?	n or more x, prefer fewer
x{n}?	exactly n x
x{}	(≡ x*) (NOT SUPPORTED) VIM
x{-}	(≡ x*?) (NOT SUPPORTED) VIM
x{-n}	(≡ x{n}?) (NOT SUPPORTED) VIM
x=	(≡ x?) (NOT SUPPORTED) VIM

Implementation restriction: The counting forms `x{n,m}`, `x{n,}`, and `x{n}` reject forms that create a minimum or maximum repetition count above 1000. Unlimited repetitions are not subject to this restriction.

	POSSESSIVE REPETITIONS
x*+	zero or more x, possessive (NOT SUPPORTED)
x++	one or more x, possessive (NOT SUPPORTED)
x?+	zero or one x, possessive (NOT SUPPORTED)
x{n,m}+	n or ... or m x, possessive (NOT SUPPORTED)
x{n,}+	n or more x, possessive (NOT SUPPORTED)
x{n}+	exactly n x, possessive (NOT SUPPORTED)

	GROUPING
(re)	numbered capturing group (submatch)
(?P<name>re)	named & numbered capturing group (submatch)
(?<name>re)	named & numbered capturing group (submatch) (NOT SUPPORTED)
(?'name're)	named & numbered capturing group (submatch) (NOT SUPPORTED)
(?:re)	non-capturing group
(?flags)	set flags within current group; non-capturing
(?flags:re)	set flags during re; non-capturing
(?#text)	comment (NOT SUPPORTED)
(?|x|y|z)	branch numbering reset (NOT SUPPORTED)
(?>re)	possessive match of re (NOT SUPPORTED)
re@>	possessive match of re (NOT SUPPORTED) VIM
%(re)	non-capturing group (NOT SUPPORTED) VIM

	FLAGS
i	case-insensitive (default false)
m	multi-line mode: ^ and $ match begin/end line in addition to begin/end text (default false)

	FLAGS
s	let . match \n (default false)
U	ungreedy: swap meaning of x* and x*?, x+ and x+?, etc (default false)

Flag syntax is `xyz` (set) or `-xyz` (clear) or `xy-z` (set `xy`, clear `z`).

	EMPTY STRINGS
^	at beginning of text or line (m=true)
$	at end of text (like \z not \Z) or line (m=true)
\A	at beginning of text
\b	at ASCII word boundary (\w on one side and \W, \A, or \z on the other)
\B	not at ASCII word boundary
\g	at beginning of subtext being searched (NOT SUPPORTED) PCRE
\G	at end of last match (NOT SUPPORTED) PERL
\Z	at end of text, or before newline at end of text (NOT SUPPORTED)
\z	at end of text
(?=re)	before text matching re (NOT SUPPORTED)
(?!re)	before text not matching re (NOT SUPPORTED)
(?<=re)	after text matching re (NOT SUPPORTED)
(?<!re)	after text not matching re (NOT SUPPORTED)
re&	before text matching re (NOT SUPPORTED) VIM
re@=	before text matching re (NOT SUPPORTED) VIM
re@!	before text not matching re (NOT SUPPORTED) VIM
re@<=	after text matching re (NOT SUPPORTED) VIM
re@<!	after text not matching re (NOT SUPPORTED) VIM
\zs	sets start of match (= \K) (NOT SUPPORTED) VIM
\ze	sets end of match (NOT SUPPORTED) VIM

	EMPTY STRINGS
\%^	beginning of file (NOT SUPPORTED) VIM
\%$	end of file (NOT SUPPORTED) VIM
\%V	on screen (NOT SUPPORTED) VIM
\%#	cursor position (NOT SUPPORTED) VIM
\%'m	mark m position (NOT SUPPORTED) VIM
\%23l	in line 23 (NOT SUPPORTED) VIM
\%23c	in column 23 (NOT SUPPORTED) VIM
\%23v	in virtual column 23 (NOT SUPPORTED) VIM

	ESCAPE SEQUENCES
\a	bell (≡ \007)
\f	form feed (≡ \014)
\t	horizontal tab (≡ \011)
\n	newline (≡ \012)
\r	carriage return (≡ \015)
\v	vertical tab character (≡ \013)
*	literal *, for any punctuation character *
\123	octal character code (up to three digits)
\x7F	hex character code (exactly two digits)
\x{10FFFF}	hex character code
\C	match a single byte even in UTF-8 mode
\Q...\E	literal text ... even if ... has punctuation
\1	backreference (NOT SUPPORTED)
\b	backspace (NOT SUPPORTED) (use \010)
\cK	control char ^K (NOT SUPPORTED) (use \001 etc)
\e	escape (NOT SUPPORTED) (use \033)

	ESCAPE SEQUENCES
\g1	backreference (NOT SUPPORTED)
\g{1}	backreference (NOT SUPPORTED)
\g{+1}	backreference (NOT SUPPORTED)
\g{-1}	backreference (NOT SUPPORTED)
\g{name}	named backreference (NOT SUPPORTED)
\g<name>	subroutine call (NOT SUPPORTED)
\g'name'	subroutine call (NOT SUPPORTED)
\k<name>	named backreference (NOT SUPPORTED)
\k'name'	named backreference (NOT SUPPORTED)
\lX	lowercase X (NOT SUPPORTED)
\ux	uppercase x (NOT SUPPORTED)
\L...\E	lowercase text ... (NOT SUPPORTED)
\K	reset beginning of $0 (NOT SUPPORTED)
\N{name}	named Unicode character (NOT SUPPORTED)
\R	line break (NOT SUPPORTED)
\U...\E	upper case text ... (NOT SUPPORTED)
\X	extended Unicode sequence (NOT SUPPORTED)
%d123	decimal character 123 (NOT SUPPORTED) VIM
%xFF	hex character FF (NOT SUPPORTED) VIM
%o123	octal character 123 (NOT SUPPORTED) VIM
%u1234	Unicode character 0x1234 (NOT SUPPORTED) VIM
%U12345678	Unicode character 0x12345678 (NOT SUPPORTED) VIM

	CHARACTER CLASS ELEMENTS
x	single character
A-Z	character range (inclusive)

	CHARACTER CLASS ELEMENTS
\d	Perl character class
[:foo:]	ASCII character class foo
\p{Foo}	Unicode character class Foo
\pF	Unicode character class F (one-letter name)

	NAMED CHARACTER CLASSES AS CHARACTER CLASS ELEMENTS
[\d]	digits (≡ \d)
[^\d]	not digits (≡ \D)
[\D]	not digits (≡ \D)
[^\D]	not not digits (≡ \d)
[[:name:]]	named ASCII class inside character class (≡ [:name:])
[^[:name:]]	named ASCII class inside negated character class (≡ [:^name:])
[\p{Name}]	named Unicode property inside character class (≡ \p{Name})
[^\p{Name}]	named Unicode property inside negated character class (≡ \P{Name})

	PERL CHARACTER CLASSES (ALL ASCII-ONLY)
\d	digits (≡ [0-9])
\D	not digits (≡ [^0-9])
\s	whitespace (≡ [\t\n\f\r])
\S	not whitespace (≡ [^\t\n\f\r])
\w	word characters (≡ [0-9A-Za-z_])
\W	not word characters (≡ [^0-9A-Za-z_])
\h	horizontal space (NOT SUPPORTED)
\H	not horizontal space (NOT SUPPORTED)
\v	vertical space (NOT SUPPORTED)
\V	not vertical space (NOT SUPPORTED)

	ASCII CHARACTER CLASSES
[[:alnum:]]	alphanumeric (≡ [0-9A-Za-z])
[[:alpha:]]	alphabetic (≡ [A-Za-z])
[[:ascii:]]	ASCII (≡ [\x00-\x7F])
[[:blank:]]	blank (≡ [\t])
[[:cntrl:]]	control (≡ [\x00-\x1F\x7F])
[[:digit:]]	digits (≡ [0-9])
[[:graph:]]	graphical (≡ `[!-~]` ≡ `[A-Za-z0-9!"#$%&'()\*+,\-./:;<=>?@[\\\]^_` ` {|}~]`)
[[:lower:]]	lower case (≡ [a-z])
[[:print:]]	printable (≡ [-~] ≡ [[:graph:]])
[[:punct:]]	punctuation (≡ [!-/:-@[-`{-~])
[[:space:]]	whitespace (≡ [\t\n\v\f\r])
[[:upper:]]	upper case (≡ [A-Z])
[[:word:]]	word characters (≡ [0-9A-Za-z_])
[[:xdigit:]]	hex digit (≡ [0-9A-Fa-f])

	UNICODE CHARACTER CLASS NAMES--GENERAL CATEGORY
C	other
Cc	control
Cf	format
Cn	unassigned code points (NOT SUPPORTED)
Co	private use
Cs	surrogate
L	letter
LC	cased letter (NOT SUPPORTED)
L&	cased letter (NOT SUPPORTED)

	UNICODE CHARACTER CLASS NAMES--GENERAL CATEGORY
Ll	lowercase letter
Lm	modifier letter
Lo	other letter
Lt	titlecase letter
Lu	uppercase letter
M	mark
Mc	spacing mark
Me	enclosing mark
Mn	non-spacing mark
N	number
Nd	decimal number
Nl	letter number
No	other number
P	punctuation
Pc	connector punctuation
Pd	dash punctuation
Pe	close punctuation
Pf	final punctuation
Pi	initial punctuation
Po	other punctuation
Ps	open punctuation
S	symbol
Sc	currency symbol
Sk	modifier symbol
Sm	math symbol

	UNICODE CHARACTER CLASS NAMES--GENERAL CATEGORY
So	other symbol
Z	separator
Zl	line separator
Zp	paragraph separator
Zs	space separator

UNICODE CHARACTER CLASS NAMES--SCRIPTS
Adlam
Ahom
Anatolian_Hieroglyphs
Arabic
Armenian
Avestan
Balinese
Bamum
Bassa_Vah
Batak
Bengali
Bhaiksuki
Bopomofo
Brahmi
Braille
Buginese
Buhid
Canadian_Aboriginal
Carian

UNICODE CHARACTER CLASS NAMES--SCRIPTS
Caucasian_Albanian
Chakma
Cham
Cherokee
Chorasmian
Common
Coptic
Cuneiform
Cypriot
Cyrillic
Deseret
Devanagari
Dives_Akuru
Dogra
Duployan
Egyptian_Hieroglyphs
Elbasan
Elymaic
Ethiopic
Georgian
Glagolitic
Gothic
Grantha
Greek
Gujarati

UNICODE CHARACTER CLASS NAMES--SCRIPTS
Gunjala_Gondi
Gurmukhi
Han
Hangul
Hanifi_Rohingya
Hanunoo
Hatran
Hebrew
Hiragana
Imperial_Aramaic
Inherited
Inscriptional_Pahlavi
Inscriptional_Parthian
Javanese
Kaithi
Kannada
Katakana
Kayah_Li
Kharoshthi
Khitan_Small_Script
Khmer
Khojki
Khudawadi
Lao
Latin

UNICODE CHARACTER CLASS NAMES--SCRIPTS
Lepcha
Limbu
Linear_A
Linear_B
Lisu
Lycian
Lydian
Mahajani
Makasar
Malayalam
Mandaic
Manichaean
Marchen
Masaram_Gondi
Medefaidrin
Meetei_Mayek
Mende_Kikakui
Meroitic_Cursive
Meroitic_Hieroglyphs
Miao
Modi
Mongolian
Mro
Multani
Myanmar

UNICODE CHARACTER CLASS NAMES--SCRIPTS
Nabataean
Nandinagari
New_Tai_Lue
Newa
Nko
Nushu
Nyiakeng_Puachue_Hmong
Ogham
Ol_Chiki
Old_Hungarian
Old_Italic
Old_North_Arabian
Old_Permic
Old_Persian
Old_Sogdian
Old_South_Arabian
Old_Turkic
Oriya
Osage
Osmanya
Pahawh_Hmong
Palmyrene
Pau_Cin_Hau
Phags_Pa
Phoenician

UNICODE CHARACTER CLASS NAMES--SCRIPTS
Psalter_Pahlavi
Rejang
Runic
Samaritan
Saurashtra
Sharada
Shavian
Siddham
SignWriting
Sinhala
Sogdian
Sora_Sompeng
Soyombo
Sundanese
Syloti_Nagri
Syriac
Tagalog
Tagbanwa
Tai_Le
Tai_Tham
Tai_Viet
Takri
Tamil
Tangut
Telugu

UNICODE CHARACTER CLASS NAMES--SCRIPTS
Thaana
Thai
Tibetan
Tifinagh
Tirhuta
Ugaritic
Vai
Wancho
Warang_Citi
Yezidi
Yi
Zanabazar_Square

	VIM CHARACTER CLASSES
\i	identifier character (NOT SUPPORTED) VIM
\I	\i except digits (NOT SUPPORTED) VIM
\k	keyword character (NOT SUPPORTED) VIM
\K	\k except digits (NOT SUPPORTED) VIM
\f	file name character (NOT SUPPORTED) VIM
\F	\f except digits (NOT SUPPORTED) VIM
\p	printable character (NOT SUPPORTED) VIM
\P	\p except digits (NOT SUPPORTED) VIM
\s	whitespace character (≡ [\t]) (NOT SUPPORTED) VIM
\S	non-white space character (≡ [^ \t]) (NOT SUPPORTED) VIM
\d	digits (≡ [0-9]) VIM
\D	not \d VIM

	VIM CHARACTER CLASSES
\x	hex digits (≡ [0-9A-Fa-f]) (NOT SUPPORTED) VIM
\X	not \x (NOT SUPPORTED) VIM
\o	octal digits (≡ [0-7]) (NOT SUPPORTED) VIM
\O	not \o (NOT SUPPORTED) VIM
\w	word character VIM
\W	not \w VIM
\h	head of word character (NOT SUPPORTED) VIM
\H	not \h (NOT SUPPORTED) VIM
\a	alphabetic (NOT SUPPORTED) VIM
\A	not \a (NOT SUPPORTED) VIM
\l	lowercase (NOT SUPPORTED) VIM
\L	not lowercase (NOT SUPPORTED) VIM
\u	uppercase (NOT SUPPORTED) VIM
\U	not uppercase (NOT SUPPORTED) VIM
_x	\x plus newline, for any x (NOT SUPPORTED) VIM
\c	ignore case (NOT SUPPORTED) VIM
\C	match case (NOT SUPPORTED) VIM
\m	magic (NOT SUPPORTED) VIM
\M	nomagic (NOT SUPPORTED) VIM
\v	verymagic (NOT SUPPORTED) VIM
\V	verynomagic (NOT SUPPORTED) VIM
\Z	ignore differences in Unicode combining characters (NOT SUPPORTED) VIM

	MAGIC
(?{code})	arbitrary Perl code (NOT SUPPORTED) PERL
(??{code})	postponed arbitrary Perl code (NOT SUPPORTED) PERL

	MAGIC
(?n)	recursive call to regexp capturing group n (NOT SUPPORTED)
(?+n)	recursive call to relative group +n (NOT SUPPORTED)
(?-n)	recursive call to relative group -n (NOT SUPPORTED)
(?C)	PCRE callout (NOT SUPPORTED) PCRE
(?R)	recursive call to entire regexp (≡ (?0)) (NOT SUPPORTED)
(?&name)	recursive call to named group (NOT SUPPORTED)
(?P=name)	named backreference (NOT SUPPORTED)
(?P>name)	recursive call to named group (NOT SUPPORTED)
(?(cond)true|false)	conditional branch (NOT SUPPORTED)
(?(cond)true)	conditional branch (NOT SUPPORTED)
(*ACCEPT)	make regexps more like Prolog (NOT SUPPORTED)
(*COMMIT)	(NOT SUPPORTED)
(*F)	(NOT SUPPORTED)
(*FAIL)	(NOT SUPPORTED)
(*MARK)	(NOT SUPPORTED)
(*PRUNE)	(NOT SUPPORTED)
(*SKIP)	(NOT SUPPORTED)
(*THEN)	(NOT SUPPORTED)
(*ANY)	set newline convention (NOT SUPPORTED)
(*ANYCRLF)	(NOT SUPPORTED)
(*CR)	(NOT SUPPORTED)
(*CRLF)	(NOT SUPPORTED)
(*LF)	(NOT SUPPORTED)
(*BSR_ANYCRLF)	set \R convention (NOT SUPPORTED) PCRE
(*BSR_UNICODE)	(NOT SUPPORTED) PCRE

Content license

NOTE

Portions of this page are modifications based on work created and shared by Chromium.org and used according to terms described in the Creative Commons Attribution 4.0 International License. The original page can be found here.

This work is licensed under a Creative Commons Attribution 4.0 International License.

See also

- Microsoft Edge Enterprise landing page

Reset Microsoft Edge data in the cloud

11/1/2022 • 2 minutes to read • Edit Online

This article describes the steps for resetting your Microsoft Edge data in the cloud.

> **NOTE**
> This article applies to Microsoft Edge version 88 or later unless otherwise noted.

Overview

There are situations in which you want to reset your Microsoft Edge data in the cloud. For example, you want to synchronize your data, but Microsoft Edge reports that it's unable to synchronize the data. Another example is to make sure that your data is removed from Microsoft's cloud. In both cases, Microsoft Edge lets you perform a cloud data reset.

Back up your favorites

Before performing a reset, we recommend that you back up your favorites. Use the following steps to back up your favorites.

1. In Microsoft Edge, select **Ctrl + Shift + O** > select the **ellipsis (...)** > select **Export favorites**.
2. Choose the file where you want to save your favorites. You can provide your own filename or use the default name that Microsoft Edge provides, "favorites_month_day_year.html". For example, "favorites_07_05_21.html". If you need to restore your favorites later, you can do so from that file.
3. Select **Save**.

Perform a reset to fix a synchronization problem

If Microsoft Edge reports that it can't synchronize your data and suggests resetting your data, perform a reset to fix the problem.

Use the following steps to do a reset.

1. First, make sure that you're signed out of Microsoft Edge on all your devices, including your mobile devices, except the device you're performing the reset on. To sign out of Microsoft Edge, select **Settings** > **Profiles** > **Sign out**. When signing out, don't select the option to clear favorites, settings, and etc. from your local device.
2. After you sign out of all your other devices, open Microsoft Edge on your desktop. Select **Settings** > **Profiles** > **Sync** > **Reset sync**. In the **Reset sync** dialog box, choose "Resume sync on this device after resetting sync", and then select **Reset**.

Perform a reset to remove your data from Microsoft's cloud

If you want to remove your data from Microsoft's cloud, use the following steps to do a reset.

1. Stop synchronization on devices except the device you're performing the reset on. In Microsoft Edge, select **Settings** > **Profiles** > **Sync** > **Turn off sync**.
2. After you stop synchronization, select **Settings** > **Profiles** > **Sync** > **Reset sync**. In the **Reset sync** dialog box, clear "Resume sync on this device after resetting sync", and then select **Reset**.

What to expect during and after a data reset

A data reset can take from a few seconds to a few minutes, depending on how much data you've stored in Microsoft's cloud. In some cases, you might see a message saying that a reset couldn't be completed and a suggestion to reset again. In this case, wait a few hours and try to reset the data again. If you're still unable to reset your data, contact Microsoft Edge Support.

After a data reset has been successfully completed, data will once again synchronize from your device if you chose to resume sync after the reset. You'll need to sign back in on your other devices if you want to sync from those devices. However, if you didn't choose to resume sync, then your Microsoft Edge data is removed from the cloud and your data will no longer synchronize.

See also

- Microsoft Edge Enterprise landing page
- Microsoft Edge Enterprise Sync

Create Microsoft Edge user data directory variables

11/1/2022 • 2 minutes to read • Edit Online

This article explains how you can use data directory variables instead of using hard-coded paths when modifying Microsoft Edge.

> **NOTE**
> This article applies to Microsoft Edge version 77 or later.

Path variables

Policies for modifying data directory paths (For example, configuring the UserDataDir or DownloadDirectory support variables). When configuring these policies, you can use variables instead of hard-coded paths. For example, to store your profile data under user local application data on Windows instead of the default location. Set the UserDataDir policy to **${local_app_data}\Edge\Profile**. On most Windows 10 installations, this path resolves to *C:\Users\<Current-user>\AppData\Local\Microsoft\Edge\Profile*.

> **NOTE**
> To view the current **Profile path**, open the **About version** page (type "edge://version"). The **Profile path** follows this format: *C:\Users\<Current-user>\AppData\Local\Microsoft\Edge\User Data\Default*.

Guidance for using path variables

Review the following guidance before using variables for paths.

- All policies that involve paths where Microsoft Edge stores different data are platform dependent. Some of these policies are available only on specific platforms, but others can be used on all platforms.
- To avoid errors caused by applications starting from different locations on different occasions, make sure that paths are absolute.
- Every variable can occur only once in a path. For most of them, this is the only meaningful way to use variables, because they resolve to absolute paths.
- Almost all policies will create the path if it doesn't exist (if possible in the existing circumstances).
- Using network locations for some policies can lead to unexpected results due to differences in how different versions/channels of Microsoft Edge handle the folder structure.

Supported path variables

Microsoft Edge supports the following path variables.

All platforms

VARIABLE	DESCRIPTION
${user_name}	The user who's using Microsoft Edge. Microsoft Edge respects SUIDs (Set owner User ID up on execution) Example: *audreysmall*
${machine_name}	The machine name, possibly including the domain name. Example: *audreysmall* or *audrey.ex.contoso.com*

Windows only

VARIABLE	DESCRIPTION
${documents}	The Documents folder for the current user. Example: *C:\Users\Administrator\Documents*
${local_app_data}	The Application Data folder for the current user. Example: *C:\Users\Administrator\AppData\Local*
${roaming_app_data}	The Roamed Application Data folder for the current user. Example: *C:\Users\Administrator\AppData\Roaming*
${profile}	The home folder for the current user. Example: *C:\Users\Administrator*
${global_app_data}	The system-wide Application Data folder. Example: *C:\AppData*
${program_files}	The Program Files folder for the current process. This folder depends on whether it's a 32-bit or 64-bit process. Example resolution: *C:\Program Files (x86)*
${windows}	The Windows folder. Example: *C:\Windows*
${client_name}	The name of the client PC connected to an RDP or Citrix session. This variable is empty if it's used from a local session. If it's used in a path, prefix it with something that's guaranteed not to be empty. Example: *C:\edge_profiles\session_${client_name}* resolves to *C:\edge_profiles\session_<ForlocalSessions>* and *C:\edge_profiles\session_<SomePCname>* for remote sessions.
${session_name}	The name of the active session. Use this name to distinguish multiple simultaneously connected remote sessions that are using a single user profile. Example: *WinSta0 for local desktop sessions*

macOS only

VARIABLE	DESCRIPTION
${users}	The folder where users' profiles are stored. Example: */Users*
${documents}	The Documents folder for the current user. Example: */Users/audreysmall/Documents*

Content license

NOTE

Portions of this page are modifications based on work created and shared by Chromium.org and used according to terms described in the Creative Commons Attribution 4.0 International License. The original page can be found here.

This work is licensed under a Creative Commons Attribution 4.0 International License.

See also

- Microsoft Edge Enterprise landing page

How to roll back Microsoft Edge to a previous version

11/1/2022 • 6 minutes to read • Edit Online

This article describes how to roll back to a previous version of Microsoft Edge using the rollback feature. To learn more about this feature, watch Video: Microsoft Edge version rollback.

> **NOTE**
> This article applies to Microsoft Edge version 86 or later.

Introduction to rollback

Rollback lets you replace your Microsoft Edge browser version with an earlier version. This feature is designed to be a safety net for enterprises deploying Microsoft Edge. It provides a way to troubleshoot issues with Microsoft Edge. The benefits of rollback are the ability to revert to previous browser version easily and quickly. Rollback reduces the potential impact that a Microsoft Edge issue has on business operations.

Before you begin

It's important to understand how the rollback feature is installed in a Microsoft Edge environment. You can deploy rollback using two different methods: manually with an MSI or by using Microsoft Edge update and Group Policy. We also encourage using a selection of Group Policies for a smoother deployment.

Recommendations

The rollback feature is meant to be a temporary fix for issues you might find in a Microsoft Edge browser update. We recommend that users install the latest version of the Microsoft Edge browser to use the protection provided by the latest security updates. Rollback to an earlier version risks exposure to known security issues.

Before temporarily rolling back your browser version, we also highly recommend that you enable Sync for all the users in your organization. If you don't turn on Sync, there's a risk of permanent browsing data loss. For more information about Sync, see Microsoft Edge Sync.

Caution

Only use rollback when necessary, there's always the risk of data loss.

Enable rollback manually with an MSI

Use the following steps to roll back manually with an MSI.

1. Disable Microsoft Edge Updates.

   > **NOTE**
   > We recommend that you install the most current Administrative templates. For more information, see Download and install the Microsoft Edge administrative template.

   - Open the local Group Policy Editor and go to *Computer Configuration>Administrative Templates>Microsoft Edge Update>Applications>Microsoft Edge>*.

- Select **Update policy override** and then select **Enabled**.
- Under **Options**, pick **Update disabled** from the Policy dropdown list.

2. Get the MSI.
   - Download the MSI for the version you want to roll back to from here.
   - Save the MSI to your desktop.
3. Run the rollback command.
   - Open the Windows command prompt with **Run as administrator**.
   - Type the following command, where: *C:\Users\username\Desktop\test*is the path to the MSI you downloaded, and FileNameis the name of the .msifile:
     ```
     C:\Users\username\Desktop\test>msiexec /I FileName.msi /qn ALLOWDOWNGRADE=1
     ```
     > **NOTE**
     > For more information about msiexec, see msiexec.
   - Close and reopen Microsoft Edgeto verify that the rollback worked. Under **Settings and more** (ALT + F), go to **Settings** and select **About Microsoft Edge**.

To deploy an MSI with Microsoft Endpoint Manager, see the Create and Deploy an Application with Configuration Manager guide. During the Create Application Wizard step, add the `ALLOW_DOWNGRADE=1` option to the Installation Program, e.g. `msiexec /I FileName.msi /qn ALLOWDOWNGRADE=1`.

Enable rollback with Microsoft Edge update and Group Policy

Use the following steps to enable rollback with Microsoft Edge update and Group Policy.

1. Open the local Group Policy Editor and go to *Computer Configuration>Administrative Templates>Microsoft Edge Update>Applications>Microsoft Edge>*.
2. Select **Rollback to target version** and then select **Enabled**.
3. Select **Target version override** and pick the browser version you want to roll back to.
4. Select **Update policy override** and then select **Enabled**. Under **Options**, pick one of the following options from the Policy dropdown list (except for **Update disabled**):
   - Always allow updates
   - Automatic silent updates only

   > **NOTE**
   > To force a group policy update, type `gpupdate /force` at the Windows administrator Command Prompt (Run as administrator).
5. Click **OK** to save the policy settings. Rollback will happen the next time Microsoft Edge Update checks for an update. If you want the update to happen sooner, you can change the Microsoft Edge Update polling interval or enable rollback using an MSI.

Common rollback errors

The following errors will prevent rollback:

- Input is an unsupported target version
- Input is a non-existent target version

- Input is incorrectly formatted

Recommended Group Policies

The following group policies and settings are highly recommended for using rollback.

Sync Group Policies

- ForceSync. Set ForceSync to enabled. This policy will force enable Sync on all Azure Active Directory (Azure AD) users. This policy is only effective for Microsoft Edge versions 86 and later.
- The *Configure the list of the types that are excluded from synchronization policy* allows admins to control what data can be synced by users.

Browser restart Group Policies

We recommend forcing a restart on users after rollback is enabled.

- Enable *Notify a user that a browser restart is recommended or required for pending updates*. Under Options, select **Required**.
- Enable *Set the time period for update notifications* and then set the desired time in milliseconds.

Snapshot

A snapshot is a version stamped copy of the user data folder. During a version upgrade, a snapshot of the previous version is made and stored in the snapshot folder. After rollback occurs, a version matched snapshot will be copied into the new user data folder and deleted from the snapshot folder. If no version matched snapshot is available upon downgrade, rollback will rely on Sync to populate user data into the new Microsoft Edge version.

The UserDataSnapshotRetentionLimit group policy allows you to set a limit for the number of snapshots that can be retained at any given time. By default, three snapshots are kept. You can configure this policy to keep from 0-5 snapshots.

Frequently asked questions

Manual MSI rollback

What generic MSI failures that can happen?

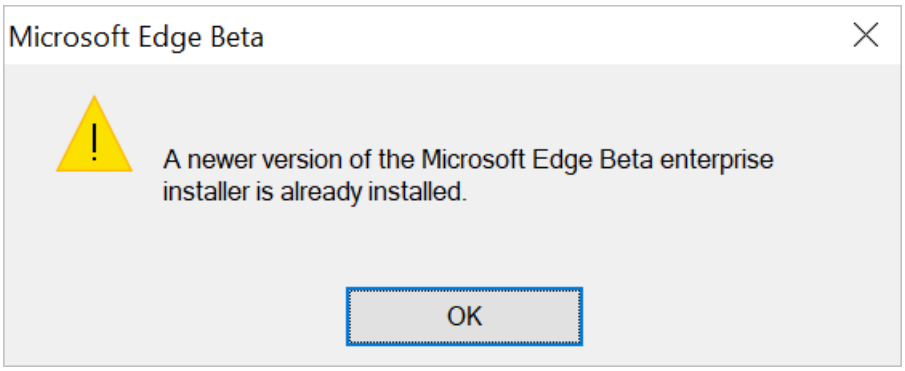
1. If the Install update group policy is disabled, rollback won't occur.

   - To use rollback, make sure Install is set to **Enabled**. When this policy is disabled, it prevents Microsoft Edge channels from being installed. For more information, see Install.

2. If Enlightenment Updates aren't present, Microsoft Edge installations will be blocked unless *Allow Microsoft Edge Side by Side browser experience* is enabled.

   - For Windows versions 1903 and 1909: If your last update was before October 2019, you may have this issue.
   - For Windows versions 1709, 1803, and 1809: If your last update was before November 2019, you may have this issue.
     For more information, see Windows updates to support the next version of Microsoft Edge

The following error message was shown after using the Command Prompt and rollback didn't occur. What's wrong?



ALLOWDOWNGRADE=1 was not executed.

Microsoft Edge Update and Group Policy rollback

I set *Rollback to target version*, enabled *Update policy override*, input my desired browser version for *Target version override*, but the browser version wasn't what I expected. What's wrong?

Some common errors that prevent rollback are:

- If Rollback to target version isn't set, rollback will not be executed.
- There are one of the following issues with the target version override setting:
  - Target version override is set to an unsupported target version.
  - Target version override is set to a non-existent target version.
  - Target version override input is incorrectly formatted.
- If Update policy override is set to "Updates disabled", Microsoft Edge Update won't accept any updates and rollback isn't executed.

I set all the group policies correctly, but rollback didn't execute. What happened?

Microsoft Edge Update hasn't run a check for updates yet. By default, auto-update checks for updates every 10 hours. You can fix this issue by changing Microsoft Edge Update's polling interval with the Auto-update check period override group policy. For more information, see the AutoUpdateCheckPeriodMinutes policy.

As an IT admin, I followed all the steps for rollback correctly. Only a portion of my user group was rolled back. Why haven't the other users been rolled back yet?

The group policy setting hasn't synced to all the clients yet. When admins set a group policy, clients don't receive these settings instantaneously. You can Force a Remote Group Policy Refresh.

See also

- Microsoft Edge Enterprise landing page
- Video: Microsoft Edge version rollback

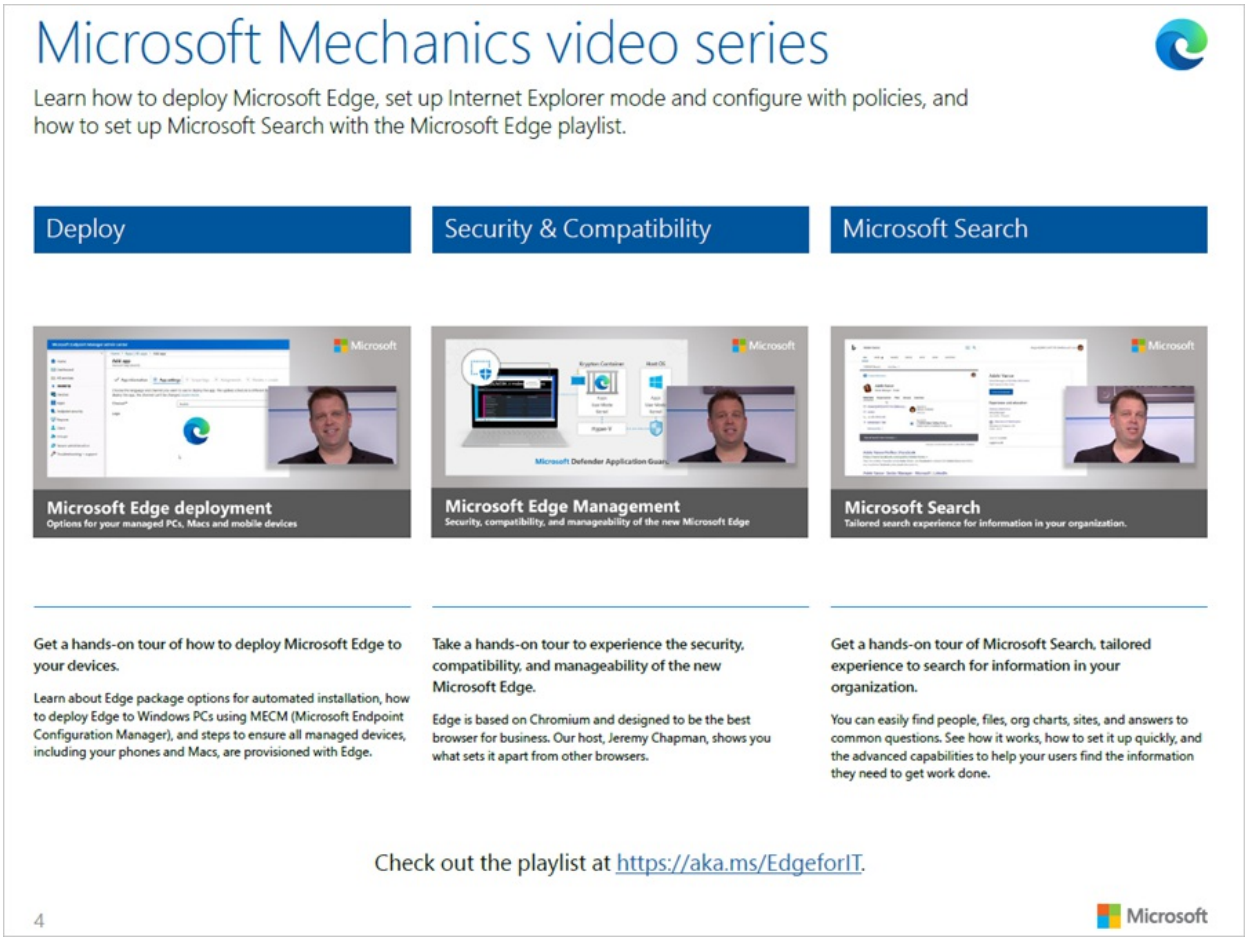
Microsoft Edge videos

11/1/2022 • 2 minutes to read • Edit Online

The videos described in this article cover many different aspects of deploying, using, and maintaining Microsoft Edge in the enterprise.

The Microsoft Mechanics video series

The Microsoft Mechanics video series, shown in the following page of the "*MSFT Edge Enterprise Deployment Guide - 2020*", is part of the Microsoft Edge collection of videos for related events and announcements, solutions, and conferences.


Microsoft Mechanics video series
Learn how to deploy Microsoft Edge, set up Internet Explorer mode and configure with policies, and how to set up Microsoft Search with the Microsoft Edge playlist.
Deploy
Security & Compatibility
Microsoft Search
Microsoft Edge deployment
Options for your managed PCs, Macs and mobile devices
Microsoft Edge Management
Security, compatibility, and manageability of the new Microsoft Edge
Microsoft Search
Tailored search experience for information in your organization.
Get a hands-on tour of how to deploy Microsoft Edge to your devices.
Learn about Edge package options for automated installation, how to deploy Edge to Windows PCs using MECM (Microsoft Endpoint Configuration Manager), and steps to ensure all managed devices, including your phones and Macs, are provisioned with Edge.
Take a hands-on tour to experience the security, compatibility, and manageability of the new Microsoft Edge.
Edge is based on Chromium and designed to be the best browser for business. Our host, Jeremy Chapman, shows you what sets it apart from other browsers.
Get a hands-on tour of Microsoft Search, tailored experience to search for information in your organization.
You can easily find people, files, org charts, sites, and answers to common questions. See how it works, how to set it up quickly, and the advanced capabilities to help your users find the information they need to get work done.
Check out the playlist at https://aka.ms/EdgeforIT.
4
Microsoft

You can view them as part of the Mechanics's Microsoft Edge playlist or on the Microsoft Edge YouTube channel alongside other videos.

See also

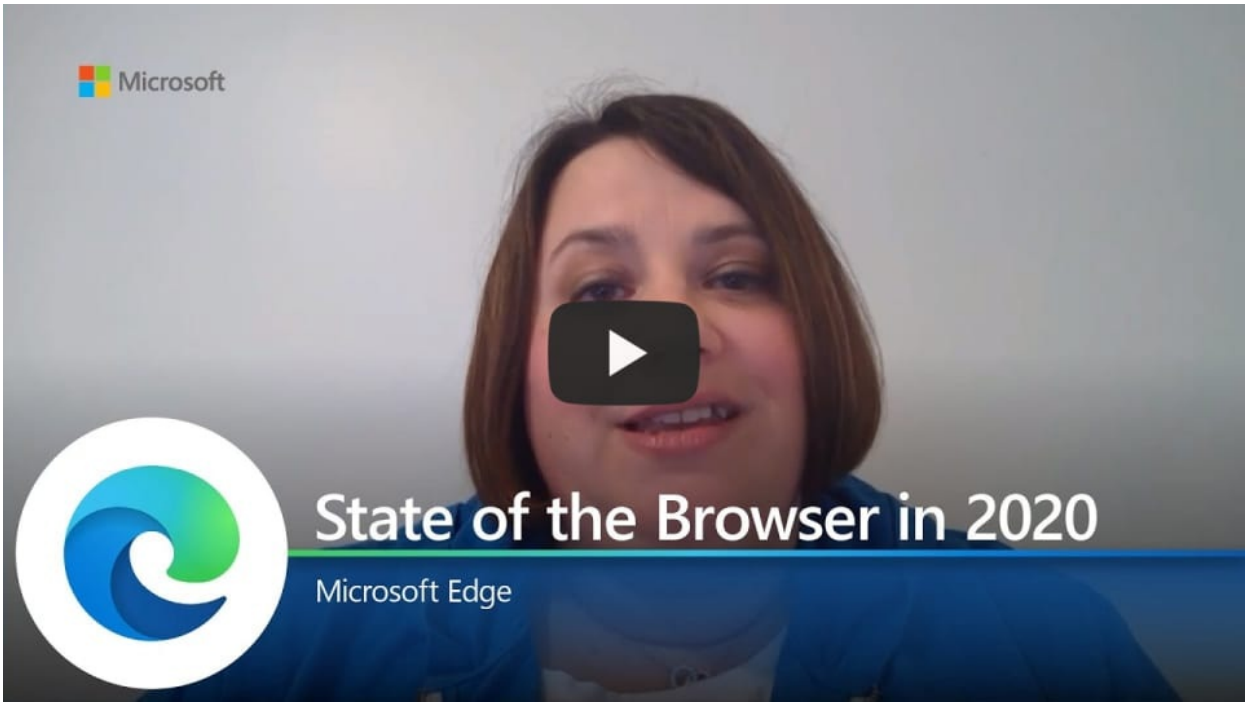
- Microsoft Edge Enterprise landing page

Video: Microsoft Edge: State of the browser 2020

11/1/2022 • 2 minutes to read • Edit Online

This video gives an overview of the key features of Microsoft Edge.

Click the next screenshot to watch the video by Colleen Williams, Senior Program Manager.



About the video

It's been an exciting year for Microsoft Edge! We've continued our mission for Microsoft Edge to be the best browser for business. Come learn about new security and productivity features and our continued integration with M365. We've been listening and learning from you and we'll share how all of that feedback fits into Microsoft Edge.

See also

- Microsoft Edge Enterprise landing page
- Microsoft Edge YouTube playlist

Video: Microsoft Edge browser isolation using Application Guard

11/1/2022 • 2 minutes to read • Edit Online

This video shows how Microsoft Edge supports browser isolation using Application Guard. Click the next screenshot to watch the video by Arunesh Chandra, Senior Program Manager, Microsoft Edge Security.

About the video

With Microsoft Edge, help reduce your enterprise's exposure to web-based attacks. Learn how Microsoft Edge supports Microsoft Defender Application Guard to use browser isolation against external threats.

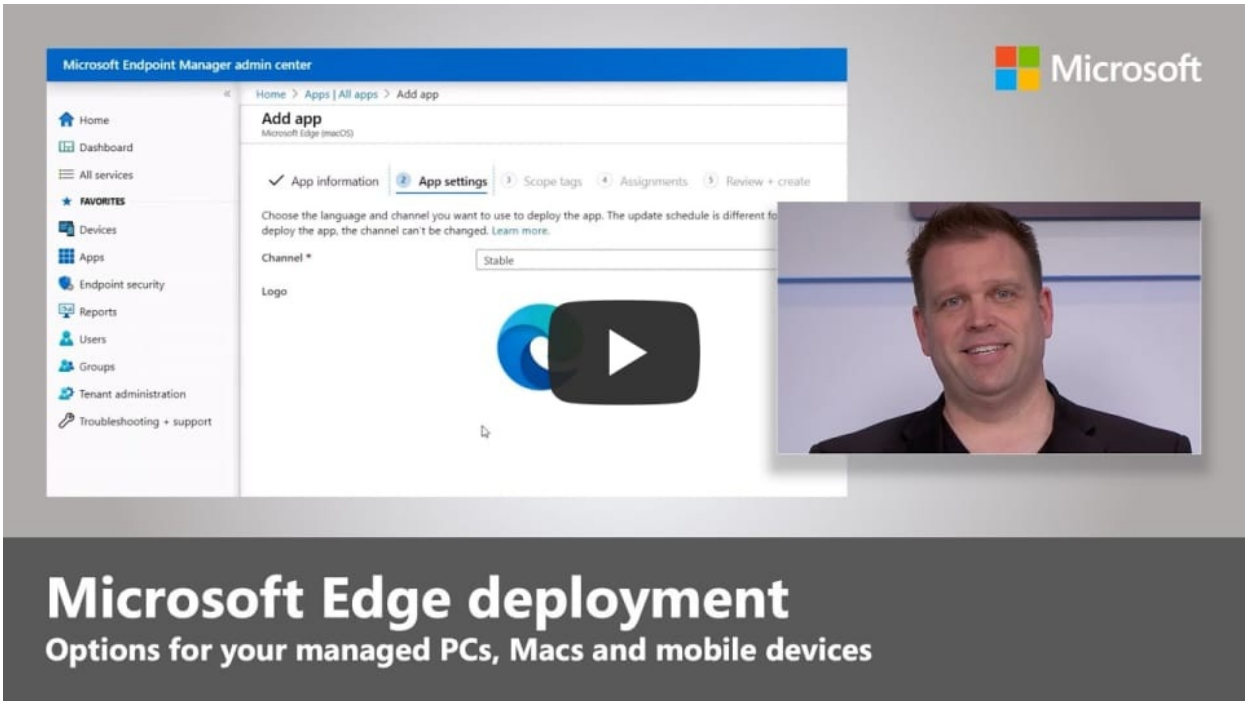
See also

- Microsoft Edge Enterprise landing page
- Microsoft Edge support for Microsoft Defender Application Guard
- Microsoft Edge YouTube playlist

Video: Deploy Microsoft Edge to hundreds or thousands of devices

11/1/2022 • 2 minutes to read • Edit Online

This video shows the steps to deploy Microsoft Edge to all your managed devices. Click the next screenshot to watch the video by Jeremy Chapman, Director Microsoft 365.


Microsoft Endpoint Manager admin center
Microsoft
Add app
Microsoft Edge deployment
Options for your managed PCs, Macs and mobile devices

About the video

See a hands-on tour of how to deploy Microsoft Edge to your devices. Learn about Microsoft Edge package options for automated installation, how to deploy Microsoft Edge to Windows PCs using Microsoft Endpoint Configuration Manager, and steps to ensure all managed devices, including your phones and Macs, are provisioned with Microsoft Edge.

See also

- Microsoft Edge Enterprise landing page
- Microsoft Edge YouTube playlist

Video: Microsoft Edge and Data loss prevention (DLP)

11/1/2022 • 2 minutes to read • Edit Online

This video shows how Microsoft Edge supports data loss prevention. Click the next screenshot to watch the video by Arunesh Chandra, Senior Program Manager, Microsoft Edge Security.

About the video

Data Loss Prevention (DLP) has never been more important than now with remote work. Learn about the native DLP capabilities in Microsoft Edge and how DLP helps you keep your data under corporate control and remain compliant.

See also

- Microsoft Edge Enterprise landing page
- Data Loss Prevention (DLP) in Microsoft Edge
- Microsoft Edge YouTube playlist

Video: Microsoft Edge and Identity

11/1/2022 • 2 minutes to read • Edit Online

This video shows how Microsoft Edge enables and supports identity for enterprise users. Click the next screenshot to watch the video by Avi Vaid, Program Manager 2.

About the video

This video describes how to configure an authenticated and personalized experience for your users. Topics include configuring sign-in, single sign-on, and multiple profiles.

See also

- Microsoft Edge Enterprise landing page
- Microsoft Edge identity support and configuration
- Microsoft Edge YouTube playlist

Video: Microsoft Edge version rollback

11/1/2022 • 2 minutes to read • Edit Online

This video shows how Microsoft Edge supports version rollback. Click the next screenshot to watch the video by Andy Zeigler, Principal Program Manager.

About the video

Version rollback lets you replace your Microsoft Edge browser version with an earlier one. Come learn how rollback in Microsoft Edge can provide your enterprise with a safety net to help reduce potential impact as you troubleshoot any issues in Microsoft Edge.

See also

- Microsoft Edge Enterprise landing page
- How to roll back Microsoft Edge to a previous version
- Microsoft Edge YouTube playlist

Video: Microsoft Edge enterprise grade PDF reader

11/1/2022 • 2 minutes to read • Edit Online

This video shows Microsoft Edge's enterprise grade PDF reader. Click the next screenshot to watch the video by Aditi Gangwar, Program Manager 2.

About the video

This video highlights the features in Microsoft Edge's built-in PDF reader. See how users can ink and highlight PDFs, open protected documents, and view and validate certificate-based Digital Signatures.

See also

- Microsoft Edge Enterprise landing page
- PDF reader in Microsoft Edge
- Microsoft Edge YouTube playlist

Video: Secure browsing on Microsoft Edge

11/1/2022 • 2 minutes to read • Edit Online

This video shows how Microsoft Edge supports secure browsing using Microsoft Defender SmartScreen. Click the next screenshot to watch the video by Eva Chen, Program Manager.

About the video

Microsoft Edge uses Microsoft Defender SmartScreen to help keep you safe while you browse. Come learn about the recent phishing and malware protection results from NSS Labs, and more about how Microsoft Defender SmartScreen brings premium enterprise security integration to Microsoft Edge.

> **TIP**
> Turn on the setting for protection from potentially unwanted apps in *edge://settings*.

See also

- Microsoft Edge Enterprise landing page
- Microsoft Edge support for Microsoft Defender SmartScreen
- Microsoft Edge YouTube playlist

Video: Microsoft Edge security, compatibility, and manageability

11/1/2022 • 2 minutes to read • Edit Online

This video shows how Microsoft Edge takes security, compatibility, and manageability to the next level. Click the next screenshot to watch the video by Jeremy Chapman, Director of Microsoft 365.

About the video

Take a hands-on tour to experience the security, compatibility, and manageability of the new Microsoft Edge. Microsoft Edge is based on Chromium and designed to be the best browser for business. Our host, Jeremy Chapman, shows you what sets it apart from other browsers. This deep dive includes:

- Security. Microsoft Edge helps protect your network and devices from malicious attacks and prevents unauthorized access and leaks of corporate data.
- Compatibility. Microsoft Edge is compatible with both the modern and legacy web.
- Manageability. Consider your update management or servicing options for Microsoft Edge.

See also

- Microsoft Edge Enterprise landing page
- Microsoft Edge security for your business
- Microsoft Edge YouTube playlist